ndaal SBOM Auditor — analysis of wto-1.12.json (SBOM #2912)

SBOM metadata

Name: wto-1.12.json * Format: spdx-json

Spec version: SPDX-2.3 * Components: 2813 * Source: upload

SHA-256: 8e2ab88522e746652beea782f8ee9f1d50ca1a6dd2111e40475a185358b9e757

Ingested: 2026-09-20T20:01:53Z

Analyzer summary

syft 1.51.0 — ok — 0 finding(s)

grype 0.118.0 — ok — 1169 finding(s)

trivy 0.74.0 — ok — 464 finding(s)

osv-scanner 2.6.0 — ok — 809 finding(s)

bomber 0.5.1 — ok — 1860 finding(s)

bomdrift bomdrift 0.9.9 — ok — 0 finding(s)

inspektr_cli inspektr 0.1.9 — ok — 303 finding(s)

shieldbom shieldbom 0.3.0 — fail — 0 finding(s)

provenant provenant-cli 1.0.10 — ok — 0 finding(s)

Findings from grype

[critical] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[critical] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[critical] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[critical] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[critical] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[critical] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

Fixed in: 0.52.0

[critical] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

Fixed in: 0.52.0

[critical] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

Fixed in: 0.52.0

[critical] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

Fixed in: 0.52.0

[critical] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

Fixed in: 0.52.0

[critical] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[critical] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[critical] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[critical] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[critical] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[critical] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[critical] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[critical] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[critical] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[critical] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[critical] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — google.golang.org/grpc@v1.67.1

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[critical] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — google.golang.org/grpc@v1.69.4

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[critical] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — google.golang.org/grpc@v1.70.0

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[critical] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — google.golang.org/grpc@v1.70.0

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[critical] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[critical] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[critical] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[critical] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[critical] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[critical] GHSA-v725-9546-7q7m (CVE-2025-21613) — github.com/go-git/go-git/v5@v5.11.0

go-git has an Argument Injection via the URL field

Fixed in: 5.13.0

[critical] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

Fixed in: 0.52.0

[critical] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

Fixed in: 0.52.0

[critical] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

Fixed in: 0.52.0

[critical] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

Fixed in: 0.52.0

[critical] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

Fixed in: 0.52.0

[critical] GHSA-x527-x647-q7gg (CVE-2026-46595) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[critical] GHSA-x527-x647-q7gg (CVE-2026-46595) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[critical] GHSA-x527-x647-q7gg (CVE-2026-46595) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[critical] GHSA-x527-x647-q7gg (CVE-2026-46595) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[critical] GHSA-x527-x647-q7gg (CVE-2026-46595) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[critical] GO-2025-3563 (CVE-2025-22871) — stdlib@go1.22.12

The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.

Fixed in: 1.23.8

[critical] GO-2025-3563 (CVE-2025-22871) — stdlib@go1.22.12

The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.

Fixed in: 1.23.8

[critical] GO-2025-3563 (CVE-2025-22871) — stdlib@go1.23.6

The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.

Fixed in: 1.23.8

[critical] GO-2025-3563 (CVE-2025-22871) — stdlib@go1.23.6

The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.

Fixed in: 1.23.8

[critical] GO-2025-3563 (CVE-2025-22871) — stdlib@go1.23.6

The net/http package improperly accepts a bare LF as a line terminator in chunked data chunk-size lines. This can permit request smuggling if a net/http server is used in conjunction with a server that incorrectly accepts a bare LF as part of a chunk-ext.

Fixed in: 1.23.8

[critical] GO-2026-4337 (CVE-2025-68121) — stdlib@go1.22.12

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Fixed in: 1.24.13

[critical] GO-2026-4337 (CVE-2025-68121) — stdlib@go1.22.12

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Fixed in: 1.24.13

[critical] GO-2026-4337 (CVE-2025-68121) — stdlib@go1.23.6

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Fixed in: 1.24.13

[critical] GO-2026-4337 (CVE-2025-68121) — stdlib@go1.23.6

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the

returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Fixed in: 1.24.13

[critical] GO-2026-4337 (CVE-2025-68121) — stdlib@go1.23.6

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Fixed in: 1.24.13

[critical] GO-2026-4337 (CVE-2025-68121) — stdlib@go1.25.5

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Fixed in: 1.24.13

[critical] GO-2026-5064 (CVE-2026-53492) — github.com/containerd/containerd@v1.7.11

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[critical] GO-2026-5064 (CVE-2026-53492) — github.com/containerd/containerd@v1.7.32

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[critical] GO-2026-5338 (CVE-2026-50195) — github.com/containerd/containerd@v1.7.11

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[critical] GO-2026-5338 (CVE-2026-50195) — github.com/containerd/containerd@v1.7.32

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[high] CVE-2023-30079 — libeconf@0.4.1

A flaw was found in the libeconf library. This issue occurs when parsing a specially crafted configuration file, causing a stack-based buffer overflow that results in a denial of service.

Fixed in: 0:0.4.1-3.el9_2

[high] CVE-2024-10963 — pam@1.5.1

A flaw was found in pam_access, where certain rules in its configuration file are mistakenly treated as hostnames. This vulnerability allows attackers to trick the system by pretending to be a trusted hostname, gaining unauthorized access. This issue poses a risk for systems that rely on this feature to control who can access certain services or terminals.

Fixed in: 0:1.5.1-22.el9_5

[high] CVE-2024-32487 — less@590

An OS command injection flaw was found in Less. Since quoting is mishandled in filename.c, opening files with attacker-controlled file names can lead to OS command execution. Exploitation requires the LESSOPEN environment variable, which is set by default in many common cases.

Fixed in: 0:590-4.el9_4

[high] CVE-2025-59375 — expat@2.5.0

A memory amplification vulnerability in libexpat allows attackers to trigger excessive dynamic memory allocations by submitting specially crafted XML input. A small input (~250 KiB) can cause the parser to allocate hundreds of megabytes, leading to denial-of-service (DoS) through memory exhaustion.

Fixed in: 0:2.5.0-5.el9_7.1

[high] CVE-2025-6020 — pam@1.5.1

A flaw was found in linux-pam. The module pam_namespace may use access user-controlled paths without proper protection, allowing local users to elevate their privileges to root via multiple symlink attacks and race conditions.

Fixed in: 0:1.5.1-26.el9_6

[high] CVE-2025-8941 — pam@1.5.1

A flaw was found in linux-pam. The pam_namespace module may improperly handle user-controlled paths, allowing local users to exploit symlink attacks and race conditions to elevate their privileges to root. This CVE provides a "complete" fix for CVE-2025-6020.

Fixed in: 0:1.5.1-26.el9_6

[high] CVE-2026-11822 — sqlite-libs@3.34.1-10.el9_8

A flaw was found in SQLite's FTS5 full-text search extension. This vulnerability involves memory corruption, specifically an out-of-bounds read and a heap buffer overflow, which can be triggered by supplying a crafted database with malformed FTS5 page data. When an FTS5 MATCH query is executed against such a database, an attacker can cause process crashes, memory exhaustion, or achieve arbitrary code execution, potentially compromising the system.

Fixed in: 0:3.34.1-11.el9_8

[high] CVE-2026-11824 — sqlite-libs@3.34.1-10.el9_8

A flaw was found in SQLite, specifically within its FTS5 full-text search extension. Attackers can exploit a heap-based buffer overflow by providing a specially crafted database. This crafted database contains malicious metadata that triggers an integer underflow during FTS5 MATCH query processing. Successful exploitation of this vulnerability can lead to a crash of the application or allow for arbitrary code execution.

Fixed in: 0:3.34.1-11.el9_8

[high] CVE-2026-14456 — openssl@1:3.5.5

A flaw was found in OpenSSL. A remote attacker could exploit this by sending a large number of QUIC Initial packets to an OpenSSL QUIC server. This can cause the server to allocate and queue new incoming channels without limit, leading to unbounded memory growth. The excessive memory consumption can result in a Denial of Service (DoS) condition, making the QUIC listener unavailable.

Fixed in: 1:3.5.8-1.el9_8

[high] CVE-2026-14456 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. A remote attacker could exploit this by sending a large number of QUIC Initial packets to an OpenSSL QUIC server. This can cause the server to allocate and queue new incoming channels without limit, leading to unbounded memory growth. The excessive memory consumption can result in a Denial of Service (DoS) condition, making the QUIC listener unavailable.

Fixed in: 1:3.5.8-1.el9_8

[high] CVE-2026-35385 — openssh@9.9p1

A flaw was found in OpenSSH. When the `scp` command is used by a root user to download a file with the legacy protocol option (`-O`) and without preserving original file permissions (`-p`), the downloaded file can be installed with elevated privileges (setuid or setgid). This unexpected behavior could allow a malicious file to execute with higher permissions than intended, posing a security risk through potential privilege escalation.

Fixed in: 0:9.9p1-7.el9_8

[high] CVE-2026-39979 — jq@1.6

A flaw was found in jq, a command line JSON processor, specifically in the libjq API. Parsing a malformed JSON input from a non-NUL-terminated buffer using the `jv_parse_sized` function can cause an out-of-bounds read, resulting in an application crash and a possible memory disclosure within the error message generated by the parser.

Fixed in: 0:1.6-19.el9_8.2

[high] CVE-2026-40164 — jq@1.6

A flaw was found in jq, a command-line JSON processor. A remote attacker could exploit this vulnerability by providing a specially crafted JSON object. This object leverages a weakness in jq's hashing algorithm, which uses a hardcoded, publicly known seed. By crafting the JSON object to cause hash collisions, an attacker can degrade the performance of JSON object hash table operations, leading to significant CPU exhaustion and a denial of service (DoS) for systems processing the malicious JSON data.

Fixed in: 0:1.6-19.el9_8.2

[high] CVE-2026-45186 — expat@2.5.0

A flaw was found in libexpat. When processing a specially crafted XML input containing a specific pattern of attributes, the parsing time increases quadratically due to checks for attribute name collisions. This consumes excessive CPU resources and eventually results in a denial of service.

Fixed in: 0:2.5.0-6.el9_8.1

[high] CVE-2026-45447 — openssl@1:3.5.5

A flaw was found in OpenSSL. When processing a specially crafted PKCS#7 or S/MIME (Secure/Multipurpose Internet Mail Extensions) signed message, a heap use-after-free vulnerability in the PKCS7_verify() function can be triggered. This occurs if the SignedData digestAlgorithms field is present as an empty ASN.1 SET, leading to incorrect memory deallocation. A remote attacker could exploit this to cause application crashes, memory corruption, or potentially achieve remote code execution.

Fixed in: 1:3.5.5-4.el9_8

[high] CVE-2026-53613 — libblkid@2.37.4-25.el9

When an /etc/fstab entry is configured with the user or users option, mount(8) validates the target path before performing the mount syscall, creating a Time-of-Check-Time-of-Use (TOCTOU) window. A local unprivileged user with write access to an ancestor directory of the mount target can swap that directory to redirect the mount to an arbitrary root-owned location, potentially escalating privileges to root.

[high] CVE-2026-53613 — libmount@2.37.4-25.el9

When an /etc/fstab entry is configured with the user or users option, mount(8) validates the target path before performing the mount syscall, creating a Time-of-Check-Time-of-Use (TOCTOU) window. A local unprivileged user with write access to an ancestor directory of the mount target can swap that directory to redirect the mount to an arbitrary root-owned location, potentially escalating privileges to root.

[high] CVE-2026-53613 — libsmartcols@2.37.4-25.el9

When an /etc/fstab entry is configured with the user or users option, mount(8) validates the target path before performing the mount syscall, creating a Time-of-Check-Time-of-Use (TOCTOU) window. A local unprivileged user with write access to an ancestor directory of the mount target can swap that directory to redirect the mount to an arbitrary root-owned location, potentially escalating privileges to root.

[high] CVE-2026-53613 — libuuid@2.37.4-25.el9

When an /etc/fstab entry is configured with the user or users option, mount(8) validates the target path before performing the mount syscall, creating a Time-of-Check-Time-of-Use (TOCTOU) window. A local unprivileged user with write access to an ancestor directory of the mount target can swap that directory to redirect the mount to an arbitrary root-owned location, potentially escalating privileges to root.

[high] CVE-2026-53613 — util-linux@2.37.4

When an /etc/fstab entry is configured with the user or users option, mount(8) validates the target path before performing the mount syscall, creating a Time-of-Check-Time-of-Use (TOCTOU) window. A local unprivileged user with write access to an ancestor directory of the mount target can swap that directory to redirect the mount to an arbitrary root-owned location, potentially escalating privileges to root.

[high] CVE-2026-59999 — openssh@9.9p1

A flaw was found in `sshd`, the OpenSSH server daemon. When `DisableForwarding=yes` is configured to prevent network traffic forwarding, it incorrectly fails to take precedence over `PermitTunnel=yes`. This allows a remote attacker to bypass intended security restrictions and establish a tunnel, potentially leading to unauthorized network access or circumvention of security policies, even when forwarding is explicitly disabled.

Fixed in: 0:9.9p1-11.el9_8

[high] CVE-2026-60002 — openssh@9.9p1

A flaw was found in OpenSSH. A remote attacker could exploit a use-after-free vulnerability on the client side when a server changes its host key during a key re-exchange. This could lead to high impact on confidentiality and integrity, and low impact on availability.

Fixed in: 0:9.9p1-9.el9_8

[high] CVE-2026-63382 — libevent@2.1.12-8.el9_4

A flaw was found in libevent. The evhttp parser in libevent's http.c component inconsistently handles HTTP Transfer-Encoding headers and chunked framing. This inconsistency allows an unauthenticated remote attacker to desynchronize request boundaries when libevent is used behind a proxy. Successful exploitation could lead to request smuggling, potentially bypassing access controls or poisoning caches.

Fixed in: 0:2.1.13-1.el9_8

[high] CVE-2026-63383 — libevent@2.1.12-8.el9_4

A flaw was found in Libevent, an event notification library. A remote attacker could exploit an out-of-bounds read vulnerability in the `decode_tag_internal()` function by sending specially crafted, attacker-controlled tagged RPC (Remote Procedure Call) data. This could lead to a denial of service, causing the process that decodes the data to crash.

Fixed in: 0:2.1.13-1.el9_8

[high] CVE-2026-63384 — libevent@2.1.12-8.el9_4

A flaw was found in Libevent. An incorrect integer conversion in the `evtag_unmarshal_header` function allows a remote attacker to provide a specially crafted payload length. This can lead to a wrapped large allocation request, resulting in a denial of service (DoS) for the affected system.

Fixed in: 0:2.1.13-1.el9_8

[high] CVE-2026-63385 — libevent@2.1.12-8.el9_4

A flaw was found in libevent. The evhttp_decode_uri_internal function in http.c decodes percent-encoded %00 bytes into literal NUL characters without rejecting them, allowing an attacker to craft a URI such as /admin/secret%00.jpg where extension-based access checks see .jpg but the server processes /admin/secret, bypassing path-based access controls. Additionally, evhttp_header_is_valid_value accepts obsolete HTTP header line folding (CRLF followed by SP/HT), which RFC 9112 states new implementations should reject, creating a header injection vector in proxy chains where the frontend rejects obs-fold but libevent accepts it. This could lead to access control bypass, header injection, or request smuggling.

Fixed in: 0:2.1.13-1.el9_8

[high] CVE-2026-63387 — libevent@2.1.12-8.el9_4

A flaw was found in Libevent, an event notification library. An off-by-one stack buffer overflow exists in the `dnsname_to_labels` function when processing a name-bearing DNS record. A remote attacker could send a specially crafted DNS server response, which may lead to a crash or corruption of the process, resulting in a denial of service or potential information disclosure and integrity impact.

Fixed in: 0:2.1.13-1.el9_8

[high] CVE-2026-63388 — libevent@2.1.12-8.el9_4

A flaw was found in Libevent. A heap out-of-bounds write vulnerability in the `bufferevent_socket_set_conn_address_` function allows an unauthenticated local peer to achieve arbitrary code execution. By connecting to an AF_UNIX listener, an attacker can overwrite critical heap data, leading to memory corruption and potentially full control over the affected system. This can severely impact the confidentiality, integrity, and availability of data and services.

Fixed in: 0:2.1.13-1.el9_8

[high] CVE-2026-66046 — expat@2.5.0

A flaw was found in the Expat XML parsing library. A remote, unauthenticated attacker can supply a specially crafted XML document to trigger quadratic algorithmic complexity in the storeAtts() function, causing excessive CPU consumption and a denial of service

[high] CVE-2026-74860 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2 with Python bindings enabled. A remote attacker could exploit this vulnerability by providing a specially crafted XML document containing a Document Type Definition (DTD) with enumerated attribute values. This triggers a double-free error in the SAX attributeDecl callback handler, where a string is freed twice. This flaw can lead to a denial of service (DoS) due to a reproducible crash in Python applications using the libxml2 SAX bindings.

[high] CVE-2026-8286 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When a new data transfer attempts to upgrade its connection using STARTTLS, it may incorrectly reuse an existing live connection. This reuse can occur even if the Transport Layer Security (TLS) configuration of the new transfer does not match the existing connection, potentially leading to an insecure connection being established.

Fixed in: 0:7.76.1-40.el9_8.5

[high] CVE-2026-8286 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When a new data transfer attempts to upgrade its connection using STARTTLS, it may incorrectly reuse an existing live connection. This reuse can occur even if the Transport Layer Security (TLS) configuration of the new transfer does not match the existing connection, potentially leading to an insecure connection being established.

Fixed in: 0:7.76.1-40.el9_8.5

[high] CVE-2026-8458 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. A logical error in the connection pooling mechanism may cause libcurl to reuse an authenticated connection for an unintended service. This could allow an application to wrongfully reuse an existing connection to the same server that was authenticated for a different service, potentially leading to unauthorized access or information disclosure.

Fixed in: 0:7.76.1-40.el9_8.7

[high] CVE-2026-8458 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. A logical error in the connection pooling mechanism may cause libcurl to reuse an authenticated connection for an unintended service. This could allow an application to wrongfully reuse an existing connection to the same server that was authenticated for a different service, potentially leading to unauthorized access or information disclosure.

Fixed in: 0:7.76.1-40.el9_8.7

[high] CVE-2026-86140 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2. A local attacker could exploit a stack-based buffer overflow in the `xmlSnprintfElements` function to achieve arbitrary code execution. This vulnerability in a fundamental system library could lead to significant system compromise if successfully exploited.

[high] CVE-2026-86145 — pcre2@10.40-6.el9

A flaw was found in PCRE2. An out-of-bounds write vulnerability exists in the `pcre2_dfa_match` function due to improper size checking when reusing cached workspace blocks. A remote attacker could exploit this by providing a specially crafted regular expression or a recursive pattern in conjunction with a small heap limit. This could lead to data corruption or potentially arbitrary code execution, compromising the integrity and availability of the system.

[high] CVE-2026-86145 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2. An out-of-bounds write vulnerability exists in the `pcre2_dfa_match` function due to improper size checking when reusing cached workspace blocks. A remote attacker could exploit this by providing a specially crafted regular expression or a recursive pattern in conjunction with a small heap limit. This could lead to data corruption or potentially arbitrary code execution, compromising the integrity and availability of the system.

[high] CVE-2026-89161 — pcre2@10.40-6.el9

A flaw was found in PCRE2, a library for processing regular expressions. The `pcre2_jit_match` function, which handles just-in-time (JIT) compilation for regular expressions, incorrectly manages memory when processing certain inputs. This memory corruption vulnerability could allow a local attacker to cause the application to crash, leading to a denial of service, or potentially execute unauthorized code.

[high] CVE-2026-89161 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2, a library for processing regular expressions. The `pcre2_jit_match` function, which handles just-in-time (JIT) compilation for regular expressions, incorrectly manages memory when processing certain inputs. This memory corruption vulnerability could allow a local attacker to cause the

application to crash, leading to a denial of service, or potentially execute unauthorized code.

[high] CVE-2026-8927 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When reusing a libcurl handle for sequential transfers with environment-variable proxy configuration, the library does not properly clear the proxy authentication state. This oversight can lead to the unintended disclosure of `Proxy-Authorization` headers to an incorrect proxy, potentially exposing sensitive authentication information to an unauthorized entity. This is an information disclosure vulnerability.

Fixed in: 0:7.76.1-40.el9_8.7

[high] CVE-2026-8927 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When reusing a libcurl handle for sequential transfers with environment-variable proxy configuration, the library does not properly clear the proxy authentication state. This oversight can lead to the unintended disclosure of `Proxy-Authorization` headers to an incorrect proxy, potentially exposing sensitive authentication information to an unauthorized entity. This is an information disclosure vulnerability.

Fixed in: 0:7.76.1-40.el9_8.7

[high] CVE-2026-9547 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When a libcurl-based application uses SCP:// or SFTP:// for transfers and employs the CURLOPT_SSH_KEYFUNCTION callback, it may silently accept an untrusted server. This occurs if the server's host key type differs from the one stored in the known_hosts file. The callback mechanism fails to enforce the host key restriction, enabling a connection to an untrusted server and risking a man-in-the-middle attack.

Fixed in: 0:7.76.1-40.el9_8.5

[high] CVE-2026-9547 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When a libcurl-based application uses SCP:// or SFTP:// for transfers and employs the CURLOPT_SSH_KEYFUNCTION callback, it may silently accept an untrusted server. This occurs if the server's host key type differs from the one stored in the known_hosts file. The callback mechanism fails to enforce the host key restriction, enabling a connection to an untrusted server and risking a man-in-the-middle attack.

Fixed in: 0:7.76.1-40.el9_8.5

[high] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — google.golang.org/grpc@v1.67.1

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

Fixed in: 1.82.2

[high] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — google.golang.org/grpc@v1.69.4

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

Fixed in: 1.82.2

[high] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — google.golang.org/grpc@v1.70.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

Fixed in: 1.82.2

[high] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — google.golang.org/grpc@v1.70.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

Fixed in: 1.82.2

[high] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — google.golang.org/grpc@v1.79.3

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

Fixed in: 1.82.2

[high] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — google.golang.org/grpc@v1.80.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

Fixed in: 1.82.2

[high] GHSA-389r-gv7p-r3rp (CVE-2026-45022) — github.com/go-git/go-git/v5@v5.11.0

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

Fixed in: 5.19.0

[high] GHSA-389r-gv7p-r3rp (CVE-2026-45022) — github.com/go-git/go-git/v5@v5.13.2

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

Fixed in: 5.19.0

[high] GHSA-3p65-76g6-3w7r (CVE-2026-33540) — github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution affected by pull-through cache credential exfiltration via www-authenticate bearer realm

Fixed in: 3.1.0

[high] GHSA-47q9-m4ww-924m (CVE-2026-48702) — github.com/sigstore/rekor@v1.2.2

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

Fixed in: 1.5.2

[high] GHSA-47q9-m4ww-924m (CVE-2026-48702) — github.com/sigstore/rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

Fixed in: 1.5.2

[high] GHSA-47q9-m4ww-924m (CVE-2026-48702) — github.com/sigstore/rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

Fixed in: 1.5.2

[high] GHSA-4c29-8rgm-jvjj (CVE-2026-33747) — github.com/moby/buildkit@v0.12.5

BuildKit's Malicious frontend can cause file escape outside of storage root

Fixed in: 0.28.1

[high] GHSA-4c29-8rgm-jvjj (CVE-2026-33747) — github.com/moby/buildkit@v0.16.0

BuildKit's Malicious frontend can cause file escape outside of storage root

Fixed in: 0.28.1

[high] GHSA-4qg8-fj49-pxjh (CVE-2025-66564) — github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing

Fixed in: 2.0.3

[high] GHSA-4qg8-fj49-pxjh (CVE-2025-66564) —

github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing

Fixed in: 2.0.3

[high] GHSA-4vrq-3vrq-g6gg (CVE-2026-33748) — github.com/moby/buildkit@v0.12.5

BuildKit Git URL subdir component can cause access to restricted files

Fixed in: 0.28.1

[high] GHSA-4vrq-3vrq-g6gg (CVE-2026-33748) — github.com/moby/buildkit@v0.16.0

BuildKit Git URL subdir component can cause access to restricted files

Fixed in: 0.28.1

[high] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — golang.org/x/oauth2@v0.12.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[high] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — golang.org/x/oauth2@v0.18.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[high] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — golang.org/x/oauth2@v0.23.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[high] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — golang.org/x/oauth2@v0.26.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[high] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — golang.org/x/oauth2@v0.26.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[high] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — github.com/go-jose/go-jose/v3@v3.0.3

Go JOSE Panics in JWE decryption

Fixed in: 3.0.5

[high] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — github.com/go-jose/go-jose/v3@v3.0.3

Go JOSE Panics in JWE decryption

Fixed in: 3.0.5

[high] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — github.com/go-jose/go-jose/v4@v4.0.5

Go JOSE Panics in JWE decryption

Fixed in: 4.1.4

[high] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — github.com/go-jose/go-jose/v4@v4.0.5

Go JOSE Panics in JWE decryption

Fixed in: 4.1.4

[high] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — github.com/go-jose/go-jose/v4@v4.0.5

Go JOSE Panics in JWE decryption

Fixed in: 4.1.4

[high] GHSA-89xv-2j6f-qhc8 (CVE-2026-33252) — github.com/modelcontextprotocol/go-sdk@v1.1.0

Cross-Site Tool Execution for HTTP Servers without Authorizatrion in github.com/modelcontextprotocol/go-sdk

Fixed in: 1.4.1

[high] GHSA-9493-h29p-rfm2 (CVE-2025-31133) — github.com/opencontainers/runc@v1.1.12

runc container escape via "masked path" abuse due to mount race conditions

Fixed in: 1.2.8

[high] GHSA-9h8m-3fm2-qjrq (CVE-2026-24051) — go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking

Fixed in: 1.40.0

[high] GHSA-9h8m-3fm2-qjrq (CVE-2026-24051) — go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking

Fixed in: 1.40.0

[high] GHSA-cgrx-mc8f-2prm (CVE-2025-52881) — github.com/opencontainers/runc@v1.1.12

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.2.8

[high] GHSA-cgrx-mc8f-2prm (CVE-2025-52881) — github.com/opencontainers/selinux@v1.11.0

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.13.0

[high] GHSA-cgrx-mc8f-2prm (CVE-2025-52881) — github.com/opencontainers/selinux@v1.11.0

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.13.0

[high] GHSA-f2g3-hh2r-cwgc (CVE-2026-35172) — github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution: stale blob access resurrection via repo-scoped redis descriptor cache invalidation

Fixed in: 3.1.0

[high] GHSA-f5f4-3hh4-f54m (CVE-2026-54167) — github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

Fixed in: 0.37.8

[high] GHSA-f5f4-3hh4-f54m (CVE-2026-54167) — github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

Fixed in: 0.37.8

[high] GHSA-f5f4-3hh4-f54m (CVE-2026-54167) — github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

Fixed in: 0.37.8

[high] GHSA-f5mr-q85p-6hh6 (CVE-2026-49478) — github.com/sigstore/fulcio@v1.4.3

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

Fixed in: 1.8.6

[high] GHSA-f5mr-q85p-6hh6 (CVE-2026-49478) — github.com/sigstore/fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

Fixed in: 1.8.6

[high] GHSA-f5mr-q85p-6hh6 (CVE-2026-49478) — github.com/sigstore/fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

Fixed in: 1.8.6

[high] GHSA-f83f-xpx7-ffpw (CVE-2025-66506) — github.com/sigstore/fulcio@v1.4.3

Fulcio allocates excessive memory during token parsing

Fixed in: 1.8.3

[high] GHSA-f83f-xpx7-ffpw (CVE-2025-66506) — github.com/sigstore/fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing

Fixed in: 1.8.3

[high] GHSA-f83f-xpx7-ffpw (CVE-2025-66506) — github.com/sigstore/fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing

Fixed in: 1.8.3

[high] GHSA-fxhp-mv3v-67qp (CVE-2026-50163) — oras.land/oras-go/v2@v2.6.1

`oras-go` tar extraction: Hardlink entry with relative Linkname escapes extract dir via process CWD resolution

Fixed in: 2.6.2

[high] GHSA-hc8v-wwc9-vgxm (CVE-2026-71556) — github.com/go-git/go-git/v5@v5.11.0

go-git: Worktree operations may follow symlinks

Fixed in: 5.19.2

[high] GHSA-hc8v-wwc9-vgxm (CVE-2026-71556) — github.com/go-git/go-git/v5@v5.13.2

go-git: Worktree operations may follow symlinks

Fixed in: 5.19.2

[high] GHSA-hcg3-q754-cr77 (CVE-2025-22869) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

Fixed in: 0.35.0

[high] GHSA-hcg3-q754-cr77 (CVE-2025-22869) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

Fixed in: 0.35.0

[high] GHSA-hcg3-q754-cr77 (CVE-2025-22869) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

Fixed in: 0.35.0

[high] GHSA-hfvc-g4fc-pqhx (CVE-2026-39883) — go.opentelemetry.io/otel/sdk@v1.34.0

opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking

Fixed in: 1.43.0

[high] GHSA-hfvc-g4fc-pqhx (CVE-2026-39883) — go.opentelemetry.io/otel/sdk@v1.34.0

opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking

Fixed in: 1.43.0

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.67.1

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.69.4

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.79.3

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.80.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-m37j-52j7-pjw7 (CVE-2026-85731) — oras.land/oras-go/v2@v2.6.1

oras-go: Arbitrary file write outside file.Store root via symlink-chain bypass in tar extraction (pushDir)

Fixed in: 2.6.2

[high] GHSA-mh63-6h87-95cp (CVE-2025-30204) — github.com/golang-jwt/jwt/v4@v4.5.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 4.5.2

[high] GHSA-mh63-6h87-95cp (CVE-2025-30204) — github.com/golang-jwt/jwt/v4@v4.5.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 4.5.2

[high] GHSA-mh63-6h87-95cp (CVE-2025-30204) — github.com/golang-jwt/jwt/v4@v4.5.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 4.5.2

[high] GHSA-mh63-6h87-95cp (CVE-2025-30204) — github.com/golang-jwt/jwt/v5@v5.2.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 5.2.2

[high] GHSA-mh63-6h87-95cp (CVE-2025-30204) — github.com/golang-jwt/jwt/v5@v5.2.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 5.2.2

[high] GHSA-p436-gjf2-799p (CVE-2025-15558) — github.com/docker/cli@v27.4.1+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

Fixed in: 29.2.0

[high] GHSA-p436-gjf2-799p (CVE-2025-15558) — github.com/docker/cli@v28.0.0+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

Fixed in: 29.2.0

[high] GHSA-p436-gjf2-799p (CVE-2025-15558) — github.com/docker/cli@v28.0.0+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

Fixed in: 29.2.0

[high] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — github.com/moby/spdystream@v0.2.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[high] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — github.com/moby/spdystream@v0.2.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[high] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — github.com/moby/spdystream@v0.4.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[high] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — github.com/moby/spdystream@v0.5.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[high] GHSA-pwhc-rpq9-4c8w (CVE-2024-25621) — github.com/containerd/containerd@v1.7.11

containerd affected by a local privilege escalation via wide permissions on CRI directory

Fixed in: 1.7.29

[high] GHSA-q382-vc8q-7jhj — github.com/modelcontextprotocol/go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

Fixed in: 1.4.1

[high] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

Fixed in: 0.52.0

[high] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

Fixed in: 0.52.0

[high] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

Fixed in: 0.52.0

[high] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

Fixed in: 0.52.0

[high] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

Fixed in: 0.52.0

[high] GHSA-qw64-3x98-g7q2 (CVE-2026-44973) — github.com/go-git/go-billy/v5@v5.5.0

go-billy has path traversal vulnerabilities

Fixed in: 5.9.0

[high] GHSA-qw64-3x98-g7q2 (CVE-2026-44973) — github.com/go-git/go-billy/v5@v5.6.2

go-billy has path traversal vulnerabilities

Fixed in: 5.9.0

[high] GHSA-qw9x-cqr3-wc7r (CVE-2025-52565) — github.com/opencontainers/runc@v1.1.12

runc container escape with malicious config due to /dev/console mount and related races

Fixed in: 1.2.8

[high] GHSA-r9px-m959-cxf4 (CVE-2025-21614) — github.com/go-git/go-git/v5@v5.11.0

go-git clients vulnerable to DoS via maliciously crafted Git server replies

Fixed in: 5.13.0

[high] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — github.com/docker/docker@v25.0.6+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — github.com/docker/docker@v27.4.1+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — github.com/docker/docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — github.com/docker/docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.67.1

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

Fixed in: 1.83.1

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.69.4

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

Fixed in: 1.83.1

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.70.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

Fixed in: 1.83.1

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.70.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

Fixed in: 1.83.1

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.79.3

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

Fixed in: 1.83.1

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.80.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

Fixed in: 1.83.1

[high] GHSA-w879-237q-wc7r (CVE-2026-39829) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

Fixed in: 0.52.0

[high] GHSA-w879-237q-wc7r (CVE-2026-39829) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

Fixed in: 0.52.0

[high] GHSA-w879-237q-wc7r (CVE-2026-39829) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

Fixed in: 0.52.0

[high] GHSA-w879-237q-wc7r (CVE-2026-39829) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

Fixed in: 0.52.0

[high] GHSA-w879-237q-wc7r (CVE-2026-39829) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

Fixed in: 0.52.0

[high] GHSA-wvj2-96wp-fq3f (CVE-2026-27896) — github.com/modelcontextprotocol/go-sdk@v1.1.0

MCP Go SDK Vulnerable to Improper Handling of Case Sensitivity

Fixed in: 1.3.1

[high] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — github.com/docker/docker@v25.0.6+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — github.com/docker/docker@v27.4.1+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — github.com/docker/docker@v28.0.0+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — github.com/docker/docker@v28.0.0+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] GHSA-xhf5-7wjv-pqxp (CVE-2026-53488) — github.com/containerd/containerd@v1.7.11

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

Fixed in: 1.7.33

[high] GHSA-xhf5-7wjv-pqxp (CVE-2026-53488) — github.com/containerd/containerd@v1.7.32

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

Fixed in: 1.7.33

[high] GHSA-xw59-hvm2-8pj6 (CVE-2026-34742) — github.com/modelcontextprotocol/go-sdk@v1.1.0

DNS Rebinding Protection Disabled by Default in Model Context Protocol Go SDK for Servers Running on Localhost

Fixed in: 1.4.0

[high] GO-2025-3849 (CVE-2025-47907) — stdlib@go1.22.12

Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.

Fixed in: 1.23.12

[high] GO-2025-3849 (CVE-2025-47907) — stdlib@go1.22.12

Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.

Fixed in: 1.23.12

[high] GO-2025-3849 (CVE-2025-47907) — stdlib@go1.23.6

Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.

Fixed in: 1.23.12

[high] GO-2025-3849 (CVE-2025-47907) — stdlib@go1.23.6

Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of another query, causing the call to Scan to return either unexpected results from the other query or an error.

Fixed in: 1.23.12

[high] GO-2025-3849 (CVE-2025-47907) — stdlib@go1.23.6

Cancelling a query (e.g. by cancelling the context passed to one of the query methods) during a call to the Scan method of the returned Rows can result in unexpected results if other queries are being made in parallel. This can result in a race condition that may overwrite the expected results with those of

another query, causing the call to Scan to return either unexpected results from the other query or an error.

Fixed in: 1.23.12

[high] GO-2025-4006 (CVE-2025-61725) — stdlib@go1.22.12

The ParseAddress function constructs domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[high] GO-2025-4006 (CVE-2025-61725) — stdlib@go1.22.12

The ParseAddress function constructs domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[high] GO-2025-4006 (CVE-2025-61725) — stdlib@go1.23.6

The ParseAddress function constructs domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[high] GO-2025-4006 (CVE-2025-61725) — stdlib@go1.23.6

The ParseAddress function constructs domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[high] GO-2025-4006 (CVE-2025-61725) — stdlib@go1.23.6

The ParseAddress function constructs domain-literal address components through repeated string concatenation. When parsing large domain-literal components, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[high] GO-2025-4007 (CVE-2025-58187) — stdlib@go1.22.12

Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.9

[high] GO-2025-4007 (CVE-2025-58187) — stdlib@go1.22.12

Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.9

[high] GO-2025-4007 (CVE-2025-58187) — stdlib@go1.23.6

Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.9

[high] GO-2025-4007 (CVE-2025-58187) — stdlib@go1.23.6

Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.9

[high] GO-2025-4007 (CVE-2025-58187) — stdlib@go1.23.6

Due to the design of the name constraint checking algorithm, the processing time of some inputs scale non-linearly with respect to the size of the certificate. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.9

[high] GO-2025-4009 (CVE-2025-61723) — stdlib@go1.22.12

The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.

Fixed in: 1.24.8

[high] GO-2025-4009 (CVE-2025-61723) — stdlib@go1.22.12

The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.

Fixed in: 1.24.8

[high] GO-2025-4009 (CVE-2025-61723) — stdlib@go1.23.6

The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.

Fixed in: 1.24.8

[high] GO-2025-4009 (CVE-2025-61723) — stdlib@go1.23.6

The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.

Fixed in: 1.24.8

[high] GO-2025-4009 (CVE-2025-61723) — stdlib@go1.23.6

The processing time for parsing some invalid inputs scales non-linearly with respect to the size of the input. This affects programs which parse untrusted PEM inputs.

Fixed in: 1.24.8

[high] GO-2025-4013 (CVE-2025-58188) — stdlib@go1.22.12

Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.8

[high] GO-2025-4013 (CVE-2025-58188) — stdlib@go1.22.12

Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.8

[high] GO-2025-4013 (CVE-2025-58188) — stdlib@go1.23.6

Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.8

[high] GO-2025-4013 (CVE-2025-58188) — stdlib@go1.23.6

Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.8

[high] GO-2025-4013 (CVE-2025-58188) — stdlib@go1.23.6

Validating certificate chains which contain DSA public keys can cause programs to panic, due to a interface cast that assumes they implement the Equal method. This affects programs which validate arbitrary certificate chains.

Fixed in: 1.24.8

[high] GO-2025-4116 (CVE-2025-47913) — golang.org/x/crypto@v0.32.0

SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.

Fixed in: 0.43.0

[high] GO-2025-4116 (CVE-2025-47913) — golang.org/x/crypto@v0.33.0

SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.

Fixed in: 0.43.0

[high] GO-2025-4116 (CVE-2025-47913) — golang.org/x/crypto@v0.33.0

SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.

Fixed in: 0.43.0

[high] GO-2025-4116 (CVE-2025-47913) — golang.org/x/crypto@v0.39.0

SSH clients receiving SSH_AGENT_SUCCESS when expecting a typed response will panic and cause early termination of the client process.

Fixed in: 0.43.0

[high] GO-2025-4155 (CVE-2025-61729) — stdlib@go1.22.12

Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.

Fixed in: 1.24.11

[high] GO-2025-4155 (CVE-2025-61729) — stdlib@go1.22.12

Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.

Fixed in: 1.24.11

[high] GO-2025-4155 (CVE-2025-61729) — stdlib@go1.23.6

Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.

Fixed in: 1.24.11

[high] GO-2025-4155 (CVE-2025-61729) — stdlib@go1.23.6

Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.

Fixed in: 1.24.11

[high] GO-2025-4155 (CVE-2025-61729) — stdlib@go1.23.6

Within HostnameError.Error(), when constructing an error string, there is no limit to the number of hosts that will be printed out. Furthermore, the error string is constructed by repeated string concatenation, leading to quadratic runtime. Therefore, a certificate provided by a malicious actor can result in excessive resource consumption.

Fixed in: 1.24.11

[high] GO-2026-4341 (CVE-2025-61726) — stdlib@go1.22.12

The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.

Fixed in: 1.24.12

[high] GO-2026-4341 (CVE-2025-61726) — stdlib@go1.22.12

The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.

Fixed in: 1.24.12

[high] GO-2026-4341 (CVE-2025-61726) — stdlib@go1.23.6

The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.

Fixed in: 1.24.12

[high] GO-2026-4341 (CVE-2025-61726) — stdlib@go1.23.6

The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.

Fixed in: 1.24.12

[high] GO-2026-4341 (CVE-2025-61726) — stdlib@go1.23.6

The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.

Fixed in: 1.24.12

[high] GO-2026-4341 (CVE-2025-61726) — stdlib@go1.25.5

The net/url package does not set a limit on the number of query parameters in a query. While the maximum size of query parameters in URLs is generally limited by the maximum request header size, the net/http.Request.ParseForm method can parse large URL-encoded forms. Parsing a large form containing many unique query parameters can cause excessive memory consumption.

Fixed in: 1.24.12

[high] GO-2026-4601 (CVE-2026-25679) — stdlib@go1.22.12

url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Fixed in: 1.25.8

[high] GO-2026-4601 (CVE-2026-25679) — stdlib@go1.22.12

url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Fixed in: 1.25.8

[high] GO-2026-4601 (CVE-2026-25679) — stdlib@go1.23.6

url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Fixed in: 1.25.8

[high] GO-2026-4601 (CVE-2026-25679) — stdlib@go1.23.6

url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Fixed in: 1.25.8

[high] GO-2026-4601 (CVE-2026-25679) — stdlib@go1.23.6

url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Fixed in: 1.25.8

[high] GO-2026-4601 (CVE-2026-25679) — stdlib@go1.25.5

url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Fixed in: 1.25.8

[high] GO-2026-4870 (CVE-2026-32283) — stdlib@go1.22.12

If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.

Fixed in: 1.25.9

[high] GO-2026-4870 (CVE-2026-32283) — stdlib@go1.22.12

If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.

Fixed in: 1.25.9

[high] GO-2026-4870 (CVE-2026-32283) — stdlib@go1.23.6

If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.

Fixed in: 1.25.9

[high] GO-2026-4870 (CVE-2026-32283) — stdlib@go1.23.6

If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.

Fixed in: 1.25.9

[high] GO-2026-4870 (CVE-2026-32283) — stdlib@go1.23.6

If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.

Fixed in: 1.25.9

[high] GO-2026-4870 (CVE-2026-32283) — stdlib@go1.25.5

If one side of the TLS connection sends multiple key update messages post-handshake in a single record, the connection can deadlock, causing uncontrolled consumption of resources. This can lead to a denial of service. This only affects TLS 1.3.

Fixed in: 1.25.9

[high] GO-2026-4887 (CVE-2026-34040) — github.com/docker/docker@v25.0.6+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[high] GO-2026-4887 (CVE-2026-34040) — github.com/docker/docker@v27.4.1+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[high] GO-2026-4887 (CVE-2026-34040) — github.com/docker/docker@v28.0.0+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[high] GO-2026-4887 (CVE-2026-34040) — github.com/docker/docker@v28.0.0+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.33.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.33.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.34.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.35.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.35.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.41.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — golang.org/x/net@v0.52.0

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 0.53.0

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.22.12

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.22.12

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.23.6

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.23.6

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.23.6

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.25.5

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.25.9

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4918 (CVE-2026-33814) — stdlib@go1.26.2

When processing HTTP/2 SETTINGS frames, transport will enter an infinite loop of writing CONTINUATION frames if it receives a SETTINGS_MAX_FRAME_SIZE with a value of 0.

Fixed in: 1.25.10

[high] GO-2026-4946 (CVE-2026-32281) — stdlib@go1.22.12

Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

Fixed in: 1.25.9

[high] GO-2026-4946 (CVE-2026-32281) — stdlib@go1.22.12

Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

Fixed in: 1.25.9

[high] GO-2026-4946 (CVE-2026-32281) — stdlib@go1.23.6

Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

Fixed in: 1.25.9

[high] GO-2026-4946 (CVE-2026-32281) — stdlib@go1.23.6

Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

Fixed in: 1.25.9

[high] GO-2026-4946 (CVE-2026-32281) — stdlib@go1.23.6

Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

Fixed in: 1.25.9

[high] GO-2026-4946 (CVE-2026-32281) — stdlib@go1.25.5

Validating certificate chains which use policies is unexpectedly inefficient when certificates in the chain contain a very large number of policy mappings, possibly causing denial of service. This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

Fixed in: 1.25.9

[high] GO-2026-4947 (CVE-2026-32280) — stdlib@go1.22.12

During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.

Fixed in: 1.25.9

[high] GO-2026-4947 (CVE-2026-32280) — stdlib@go1.22.12

During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.

Fixed in: 1.25.9

[high] GO-2026-4947 (CVE-2026-32280) — stdlib@go1.23.6

During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.

Fixed in: 1.25.9

[high] GO-2026-4947 (CVE-2026-32280) — stdlib@go1.23.6

During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.

Fixed in: 1.25.9

[high] GO-2026-4947 (CVE-2026-32280) — stdlib@go1.23.6

During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.

Fixed in: 1.25.9

[high] GO-2026-4947 (CVE-2026-32280) — stdlib@go1.25.5

During chain building, the amount of work that is done is not correctly limited when a large number of intermediate certificates are passed in VerifyOptions.Intermediates, which can lead to a denial of service. This affects both direct users of crypto/x509 and users of crypto/tls.

Fixed in: 1.25.9

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.22.12

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.22.12

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.23.6

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.23.6

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.23.6

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.25.5

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.25.9

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4970 (CVE-2026-39822) — stdlib@go1.26.2

On Unix systems, opening a file in an os.Root improperly follows symlinks to locations outside of the Root when the final path component of the a path is a symbolic link and the path ends in /. For example, 'root.Open("symlink/")' will open "symlink" even when "symlink" is a symbolic link pointing outside of the root.

Fixed in: 1.25.12

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.22.12

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.22.12

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.23.6

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.23.6

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.23.6

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.25.5

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.25.9

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4971 (CVE-2026-39836) — stdlib@go1.26.2

The Dial and LookupPort functions panic on Windows when provided with an input containing a NUL (0).

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.22.12

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.22.12

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.23.6

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.23.6

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.23.6

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.25.5

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.25.9

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4977 (CVE-2026-42499) — stdlib@go1.26.2

Pathological inputs could cause DoS through consumePhrase when parsing an email address according to RFC 5322.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.22.12

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.22.12

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.23.6

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.23.6

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.23.6

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.25.5

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.25.9

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4981 (CVE-2026-33811) — stdlib@go1.26.2

When using LookupCNAME with the cgo DNS resolver, a very long CNAME response can trigger a double-free of C memory and a crash.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.22.12

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.22.12

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.23.6

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.23.6

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.23.6

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.25.5

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.25.9

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-4986 (CVE-2026-39820) — stdlib@go1.26.2

Well-crafted inputs reaching ParseAddress, ParseAddressList, and ParseDate were able to trigger excessive CPU exhaustion and memory allocations.

Fixed in: 1.25.10

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.33.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.33.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.34.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.35.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.35.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII

hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.41.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — golang.org/x/net@v0.52.0

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 0.55.0

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.22.12

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.22.12

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.23.6

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.23.6

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name

"example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.23.6

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.25.5

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.25.9

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.26.2

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.26.5

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5026 (CVE-2026-39821) — stdlib@go1.26.5

The ToASCII and ToUnicode functions incorrectly accept Punycode-encoded labels that decode to an ASCII-only label. For example, ToUnicode("xn--example-.com") incorrectly returns the name "example.com" rather than an error. This behavior can lead to privilege escalation in programs using the idna package. For example, a program which performs privilege checks on the ASCII hostname may reject "example.com" but permit "xn--example-.com". If that program subsequently converts the ASCII hostname to Unicode, it will inadvertently permits access to the Unicode name "example.com".

Fixed in: 1.25.13

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.22.12

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.22.12

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.23.6

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.23.6

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.23.6

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.25.5

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.25.9

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5037 (CVE-2026-27145) — stdlib@go1.26.2

(*x509.Certificate).VerifyHostname previously called matchHostnames in a loop over all DNS Subject Alternative Name (SAN) entries. This caused strings.Split(host, ".") to execute repeatedly on the same input hostname. With a large DNS SAN list, verification costs scaled quadratically based on the number of SAN entries multiplied by the hostname's label count. Because x509.Verify validates hostnames before building the certificate chain, this overhead occurred even for untrusted certificates.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.22.12

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.22.12

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.23.6

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.23.6

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.23.6

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.25.5

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume

excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.25.9

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5038 (CVE-2026-42504) — stdlib@go1.26.2

Decoding a maliciously-crafted MIME header containing many invalid encoded-words can consume excessive CPU.

Fixed in: 1.25.11

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.33.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.33.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.34.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.35.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.35.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.41.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.52.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.55.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — golang.org/x/net@v0.55.0

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 0.56.0

[high] GO-2026-5942 (CVE-2026-46600) — stdlib@go1.26.2

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 1.26.6

[high] GO-2026-5942 (CVE-2026-46600) — stdlib@go1.26.5

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 1.26.6

[high] GO-2026-5942 (CVE-2026-46600) — stdlib@go1.26.5

Parsing an invalid SVCB or HTTPS RR can panic when the size of a parameter value overflows the message buffer.

Fixed in: 1.26.6

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.21.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.21.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.22.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.22.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.22.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.26.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.35.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.37.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5970 (CVE-2026-56852) — golang.org/x/text@v0.38.0

A norm.Iter can enter an infinite loop when handling input containing invalid UTF-8 bytes.

Fixed in: 0.39.0

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.22.12

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.22.12

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.23.6

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.23.6

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.23.6

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.25.5

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.25.9

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.26.2

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.26.5

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-5972 (CVE-2026-33818) — stdlib@go1.26.5

Enforce a recursion limit in Unmarshal to prevent stack exhaustion when parsing deeply-nested, recursive structures.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.22.12

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.22.12

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.23.6

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.23.6

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.23.6

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.25.5

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.25.9

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.26.2

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.26.5

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6088 (CVE-2026-56859) — stdlib@go1.26.5

Previously, DecodeElement would reset the depth counter causing it to never fire; this could lead to stack exhaustion.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.22.12

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.22.12

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.23.6

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.23.6

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.23.6

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.25.5

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.25.9

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new

connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.26.2

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.26.5

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6089 (CVE-2026-56853) — stdlib@go1.26.5

When a server is configured to support unencrypted HTTP/2, it reads a few bytes from each new connection to see if they contain the HTTP/2 client preface. ReadHeaderTimeout is unexpectedly not being applied when doing this.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.22.12

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.22.12

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.23.6

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.23.6

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.23.6

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.25.5

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.25.9

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.26.2

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.26.5

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6090 (CVE-2026-56862) — stdlib@go1.26.5

Handshake messages, such as KeyUpdate, are always considered as state-advancing, regardless of whether a handshake has been completed or not. As a result, a malicious client can keep sending KeyUpdate messages to force the server to keep performing key derivation operations indefinitely.

Fixed in: 1.25.13

[high] GO-2026-6179 (CVE-2026-56865) — golang.org/x/mod@v0.22.0

A malicious GOPROXY was previously capable of forging up to two sumdb tiles that allow for a requested module to bypass the GOSUMDB check and persist attacker-controlled module content to a local Go module cache. This attack allows for a malicious GOPROXY to serve malicious module content that cannot be detected by evaluating the transparency log. All tiles are now correctly verified against their parents. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6179 (CVE-2026-56865) — golang.org/x/mod@v0.22.0

A malicious GOPROXY was previously capable of forging up to two sumdb tiles that allow for a requested module to bypass the GOSUMDB check and persist attacker-controlled module content to a local Go module cache. This attack allows for a malicious GOPROXY to serve malicious module content that cannot be detected by evaluating the transparency log. All tiles are now correctly verified against their parents. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6179 (CVE-2026-56865) — golang.org/x/mod@v0.25.0

A malicious GOPROXY was previously capable of forging up to two sumdb tiles that allow for a requested module to bypass the GOSUMDB check and persist attacker-controlled module content to a local Go module cache. This attack allows for a malicious GOPROXY to serve malicious module content that cannot be detected by evaluating the transparency log. All tiles are now correctly verified against their parents. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6179 (CVE-2026-56865) — golang.org/x/mod@v0.33.0

A malicious GOPROXY was previously capable of forging up to two sumdb tiles that allow for a requested module to bypass the GOSUMDB check and persist attacker-controlled module content to a local Go module cache. This attack allows for a malicious GOPROXY to serve malicious module content that cannot be detected by evaluating the transparency log. All tiles are now correctly verified against their parents. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6180 (CVE-2026-56864) — golang.org/x/mod@v0.22.0

A malicious GOSUMDB was capable of serving arbitrary module content not contained within the transparency log. This attack allows for a coordinating GOPROXY and GOSUMDB to serve a client malicious module content that cannot be detected by evaluating the transparency log. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6180 (CVE-2026-56864) — golang.org/x/mod@v0.22.0

A malicious GOSUMDB was capable of serving arbitrary module content not contained within the transparency log. This attack allows for a coordinating GOPROXY and GOSUMDB to serve a client malicious module content that cannot be detected by evaluating the transparency log. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6180 (CVE-2026-56864) — golang.org/x/mod@v0.25.0

A malicious GOSUMDB was capable of serving arbitrary module content not contained within the transparency log. This attack allows for a coordinating GOPROXY and GOSUMDB to serve a client malicious module content that cannot be detected by evaluating the transparency log. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6180 (CVE-2026-56864) — golang.org/x/mod@v0.33.0

A malicious GOSUMDB was capable of serving arbitrary module content not contained within the transparency log. This attack allows for a coordinating GOPROXY and GOSUMDB to serve a client malicious module content that cannot be detected by evaluating the transparency log. In order to determine if you have been affected: rm -r go.sum go.work.sum vendor/ && go mod tidy

Fixed in: 0.40.0

[high] GO-2026-6303 (CVE-2026-56854) — golang.org/x/crypto@v0.32.0

The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The

check is now applied to the Permissions returned by any authentication callback.

Fixed in: 0.55.0

[high] GO-2026-6303 (CVE-2026-56854) — golang.org/x/crypto@v0.33.0

The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The check is now applied to the Permissions returned by any authentication callback.

Fixed in: 0.55.0

[high] GO-2026-6303 (CVE-2026-56854) — golang.org/x/crypto@v0.33.0

The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The check is now applied to the Permissions returned by any authentication callback.

Fixed in: 0.55.0

[high] GO-2026-6303 (CVE-2026-56854) — golang.org/x/crypto@v0.39.0

The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The check is now applied to the Permissions returned by any authentication callback.

Fixed in: 0.55.0

[high] GO-2026-6303 (CVE-2026-56854) — golang.org/x/crypto@v0.49.0

The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The check is now applied to the Permissions returned by any authentication callback.

Fixed in: 0.55.0

[high] GO-2026-6303 (CVE-2026-56854) — golang.org/x/crypto@v0.53.0

The source-address critical option in the Permissions returned by an authentication callback was only enforced for the PublicKeyCallback and VerifiedPublicKeyCallback paths, extending the fix for CVE-2026-46595. Permissions returned by the PasswordCallback, KeyboardInteractiveCallback, NoClientAuthCallback, and GSSAPIWithMICConfig.AllowLogin callbacks were not validated against the client's remote address, so a source-address restriction set by those callbacks was silently ignored. The check is now applied to the Permissions returned by any authentication callback.

Fixed in: 0.55.0

[high] GO-2026-6354 (CVE-2026-78662) — golang.org/x/crypto@v0.32.0

Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add

an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.

Fixed in: 0.56.0

[high] GO-2026-6354 (CVE-2026-78662) — golang.org/x/crypto@v0.33.0

Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.

Fixed in: 0.56.0

[high] GO-2026-6354 (CVE-2026-78662) — golang.org/x/crypto@v0.33.0

Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.

Fixed in: 0.56.0

[high] GO-2026-6354 (CVE-2026-78662) — golang.org/x/crypto@v0.39.0

Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.

Fixed in: 0.56.0

[high] GO-2026-6354 (CVE-2026-78662) — golang.org/x/crypto@v0.49.0

Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.

Fixed in: 0.56.0

[high] GO-2026-6354 (CVE-2026-78662) — golang.org/x/crypto@v0.53.0

Previously, a channel registered in the mux's chanList is not usable until it is established. A malicious peer was able flood the channel's incomingRequests, deadlocking the entire connection. Now, we add an atomic established state, set when a channel becomes usable. Until such a time, handlePacket drops every packet other than the open confirmation/failure, without blocking and without tearing down the connection.

Fixed in: 0.56.0

[high] GO-2026-6355 (CVE-2026-56855) — golang.org/x/crypto@v0.32.0

Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.

Fixed in: 0.56.0

[high] GO-2026-6355 (CVE-2026-56855) — golang.org/x/crypto@v0.33.0

Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.

Fixed in: 0.56.0

[high] GO-2026-6355 (CVE-2026-56855) — golang.org/x/crypto@v0.33.0

Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.

Fixed in: 0.56.0

[high] GO-2026-6355 (CVE-2026-56855) — golang.org/x/crypto@v0.39.0

Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.

Fixed in: 0.56.0

[high] GO-2026-6355 (CVE-2026-56855) — golang.org/x/crypto@v0.49.0

Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.

Fixed in: 0.56.0

[high] GO-2026-6355 (CVE-2026-56855) — golang.org/x/crypto@v0.53.0

Previously, after a channel has been established, a malicious peer could send crafted messages that would deadlock the entire connection. Now, we handle all RFC 4254 channel messages; global requests are handled explicitly. Then, treat all other messages as a protocol error and tear the connection down instead of buffering and blocking.

Fixed in: 0.56.0

[medium] CVE-2005-2541 — tar@2:1.34

A flaw was found in tar utility that can allow the root user to extract files with preserved setuid and setgid permissions without any warning. This behavior can lead to the creation of malicious setuid executables owned by root from a crafted tar file, posing significant security risks.

[medium] CVE-2022-46663 — less@590

A vulnerability was found in less. This flaw allows crafted data to result in "less -R" not filtering ANSI escape sequences sent to the terminal.

Fixed in: 0:590-2.el9_2

[medium] CVE-2022-48303 — tar@2:1.34

A flaw was found in the Tar package. When attempting to read files with old V7 tar format with a specially crafted checksum, an invalid memory read may occur. An attacker could possibly use this issue to expose sensitive information or cause a crash.

Fixed in: 2:1.34-6.el9_1

[medium] CVE-2022-48624 — less@590

A flaw was found in less. The close_altfile() function in filename.c omits shell_quote calls for LESSCLOSE, a command line to invoke the optional input postprocessor. This issue could lead to an OS command injection vulnerability and arbitrary command execution on the host operating system.

Fixed in: 0:590-3.el9_3

[medium] CVE-2023-22652 — libeconf@0.4.1

A flaw was found in the libeconf library. This issue occurs when parsing a specially crafted configuration file, causing a stack-based buffer overflow, resulting in a denial of service.

Fixed in: 0:0.4.1-3.el9_2

[medium] CVE-2023-29491 — ncurses@6.2

A vulnerability was found in ncurses and occurs when used by a setuid application. This flaw allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.

Fixed in: 0:6.2-10.20210508.el9

[medium] CVE-2023-30571 — libarchive@3.5.3-11.el9_8

A vulnerability was found in libarchive. This issue can cause a race condition in a multi-threaded use of archive_write_disk_header() on posix based systems, which could allow implicit directory creation with permissions 777, without sticky bit, which means any low privileged user on the system can delete and rename files inside those directories.

[medium] CVE-2023-31486 — perl-HTTP-Tiny@0.076

A vulnerability was found in Tiny, where a Perl core module and standalone CPAN package, does not verify TLS certificates by default. Users need to explicitly enable certificate verification with the verify_SSL=>1 flag to ensure secure HTTPS connections. This oversight can potentially expose applications to man-in-the-middle (MITM) attacks, where an attacker might intercept and manipulate data transmitted between the client and server.

Fixed in: 0:0.076-461.el9

[medium] CVE-2023-51767 — openssh@9.9p1

An authentication bypass vulnerability was found in a modified version of OpenSSH. When common types of DRAM memory are used, it might allow row hammer attacks because the integer value of authenticated authpassword does not resist flips of a single bit. Exploiting a Rowhammer-style attack to flip bits in memory, forces successful authentication by setting the return code to 0.

[medium] CVE-2023-52425 — expat@2.5.0

A flaw was found in Expat (libexpat). When parsing a large token that requires multiple buffer fills to complete, Expat has to re-parse the token from start numerous times. This process may trigger excessive resource consumption, leading to a denial of service.

Fixed in: 0:2.5.0-1.el9_3.1

[medium] CVE-2024-10041 — pam@1.5.1

A vulnerability was found in PAM. The secret information is stored in memory, where the attacker can trigger the victim program to execute by sending characters to its standard input (stdin). As this occurs, the attacker can train the branch predictor to execute an ROP chain speculatively. This flaw could result in leaked passwords, such as those found in /etc/shadow while performing authentications.

Fixed in: 0:1.5.1-21.el9_5

[medium] CVE-2024-22365 — pam@1.5.1

A vulnerability was found in Linux PAM. An unprivileged user that is not yet in a corresponding mount namespace with ~/tmp mounted as a polyinstantiated dir can place a FIFO there, and a subsequent attempt to login as this user with `pam_namespace` configured will cause the `openat()` in `protect_dir()` to block the attempt, causing a local denial of service.

Fixed in: 0:1.5.1-19.el9

[medium] CVE-2024-23337 — jq@1.6

A flaw was found in jq, a command line JSON processor. An integer overflow can occur when attempting to assign a value using an array index of 2147483647 or when creating an array with 2147483647 elements, the maximum value for a 32-bit signed integer. This issue causes out-of-bounds memory access and results in a denial of service.

Fixed in: 0:1.6-17.el9_6.2

[medium] CVE-2024-28757 — expat@2.5.0

An XML Entity Expansion flaw was found in libexpat. This flaw allows an attacker to cause a denial of service when there is an isolated use of external parsers.

Fixed in: 0:2.5.0-2.el9_4

[medium] CVE-2024-45490 — expat@2.5.0

A flaw was found in libexpat's xmlparse.c component. This vulnerability allows an attacker to cause improper handling of XML data by providing a negative length value to the XML_ParseBuffer function.

Fixed in: 0:2.5.0-2.el9_4.1

[medium] CVE-2024-45491 — expat@2.5.0

An issue was found in libexpat’s internal dtdCopy function in xmlparse.c, It can have an integer overflow for nDefaultAtts on 32-bit platforms where UINT_MAX equals SIZE_MAX.

Fixed in: 0:2.5.0-2.el9_4.1

[medium] CVE-2024-45492 — expat@2.5.0

A flaw was found in libexpat's internal nextScaffoldPart function in xmlparse.c. It can have an integer overflow for m_groupSize on 32-bit platforms where UINT_MAX equals SIZE_MAX.

Fixed in: 0:2.5.0-2.el9_4.1

[medium] CVE-2024-50602 — expat@2.5.0

A security issue was found in Expat (libexpat). A crash can be triggered in the XML_ResumeParser function due to XML_StopParser's ability to stop or suspend an unstarted parser, which can lead to a denial of service.

Fixed in: 0:2.5.0-3.el9_5.1

[medium] CVE-2024-8176 — expat@2.5.0

A stack overflow vulnerability exists in the libexpat library due to the way it handles recursive entity expansion in XML documents. When parsing an XML document with deeply nested entity references, libexpat can be forced to recurse indefinitely, exhausting the stack space and causing a crash. This issue could lead to denial of service (DoS) or, in some cases, exploitable memory corruption, depending on the environment and library usage.

Fixed in: 0:2.5.0-5.el9_6

[medium] CVE-2025-13034 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When configured to use public key pinning with QUIC connections and

GnuTLS, and with standard certificate verification explicitly disabled, curl could bypass the intended public key check. This oversight allows a malicious server to impersonate a legitimate one, potentially leading to unauthorized access or information disclosure due to a failure in verifying the server's identity.

[medium] CVE-2025-13034 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When configured to use public key pinning with QUIC connections and GnuTLS, and with standard certificate verification explicitly disabled, curl could bypass the intended public key check. This oversight allows a malicious server to impersonate a legitimate one, potentially leading to unauthorized access or information disclosure due to a failure in verifying the server's identity.

[medium] CVE-2025-14017 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When performing multi-threaded LDAPS (Lightweight Directory Access Protocol Secure) transfers, changes to Transport Layer Security (TLS) options in one thread could inadvertently apply globally, affecting other concurrent transfers. This could lead to unintended security posture changes, such as disabling certificate verification for other threads. This vulnerability can result in a security bypass, where expected security checks are not performed.

[medium] CVE-2025-14017 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When performing multi-threaded LDAPS (Lightweight Directory Access Protocol Secure) transfers, changes to Transport Layer Security (TLS) options in one thread could inadvertently apply globally, affecting other concurrent transfers. This could lead to unintended security posture changes, such as disabling certificate verification for other threads. This vulnerability can result in a security bypass, where expected security checks are not performed.

[medium] CVE-2025-14104 — util-linux@2.37.4

A flaw was found in util-linux. This vulnerability allows a heap buffer overread when processing 256-byte usernames, specifically within the `setpwnam()` function, affecting SUID (Set User ID) login-utils utilities writing to the password database.

Fixed in: 0:2.37.4-21.el9_7

[medium] CVE-2025-32728 — openssh@9.9p1

A flaw was found in OpenSSH. In affected versions of sshd, the DisableForwarding directive does not fully adhere to the intended functionality as documented. Specifically, it fails to disable X11 and agent forwarding, which may allow unintended access under certain configurations.

[medium] CVE-2025-45582 — tar@2:1.34

A flaw was found in GNU Tar. An attacker could exploit this vulnerability by providing two specially crafted TAR archives, if those archives were extracted in the same directory. The first archive contains a symbolic link that points to a critical directory. The second archive, when extracted, uses this symbolic link to overwrite sensitive files on the system, bypassing existing directory traversal protections. This could lead to unauthorized file modification or, in some cases, privilege escalation.

Fixed in: 2:1.34-9.el9_7

[medium] CVE-2025-48060 — jq@1.6

A flaw was found in jq, a command line JSON processor. A specially crafted input can cause a heap-based buffer over-read when formatting an empty string because it was not properly null-terminated, causing a crash and resulting in a denial of service.

Fixed in: 0:1.6-17.el9_6.2

[medium] CVE-2025-48386 — git@2.52.0

A credential handling flaw has been discovered in git. The wincred credential helper uses a static buffer (target) as a unique key for storing and comparing against internal storage. This credential helper does not properly bounds check the available space remaining in the buffer before appending to it with wcsncat(), which can lead to buffer overflows.

[medium] CVE-2025-60753 — libarchive@3.5.3-11.el9_8

A vulnerability in apply_substitution() function in libarchive's bsdtar allows crafted -s substitution rules to repeatedly match a zero-length substring and append replacements without advancing the input pointer. When the rule uses the global /g flag (or an explicitly empty pattern), this leads to unbounded output allocation and eventual process OOM (Denial of Service). Upgrade to libarchive 3.8.1 or apply a patch that prevents zero-length match loops or rejects empty patterns.

[medium] CVE-2025-64118 — tar@2:1.34

A flaw was found in node-tar, a Tar utility for Node.js. This vulnerability allows a local attacker to potentially disclose sensitive information. When the .t (or .list) function is used with { sync: true } to read tar entry contents, and the tar file is concurrently modified on disk to a smaller size, the function may return uninitialized memory contents. This could lead to the exposure of arbitrary data.

[medium] CVE-2025-68972 — gnupg2@2.3.3-5.el9_7

A flaw was found in GnuPG. An adversary can exploit this vulnerability by crafting a signed message that includes a form feed character (\f) at the end of a plaintext line. This allows the adversary to append additional, unsigned text to the message while the signature verification still reports success. This issue leads to an integrity bypass, potentially enabling the spoofing of signed communications.

[medium] CVE-2026-0990 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2, an XML parsing library. This uncontrolled recursion vulnerability occurs in the xmlCatalogXMLResolveURI function when an XML catalog contains a delegate URI entry that references itself. A remote attacker could exploit this configuration-dependent issue by providing a specially crafted XML catalog, leading to infinite recursion and call stack exhaustion. This ultimately results in a segmentation fault, causing a Denial of Service (DoS) by crashing affected applications.

[medium] CVE-2026-11850 — krb5-libs@1.21.1-10.el9_8

An integer underflow vulnerability was found in MIT krb5 in the berval2tl_data() function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c. The function performs an unsigned subtraction (bv_len - 2) without a prior bounds check. When bv_len is 0 or 1, the subtraction wraps to a large value which is then truncated to uint16_t, yielding 0xFFFE (65534) or 0xFFFF (65535). The subsequent malloc succeeds and memcpy reads up to 65534 bytes from a 0-1 byte buffer, resulting in a heap out-of-bounds read. The attack vector involves a malicious or compromised LDAP KDB backend returning a krbExtraData attribute with bv_len < 2, triggering the underflow when the KDC or kadmind reads principal data.

[medium] CVE-2026-11856 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When `libcurl` performs a transfer to an HTTP origin using Digest authentication and then reuses the same connection handle for a subsequent transfer to a different origin, it may incorrectly send the authentication header intended for the first origin to the second. This could lead to unintended information disclosure, potentially allowing an attacker to gain unauthorized access to sensitive data.

[medium] CVE-2026-11856 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When `libcurl` performs a transfer to an HTTP origin using Digest authentication and then reuses the same connection handle for a subsequent transfer to a different origin, it may incorrectly send the authentication header intended for the first origin to the second. This

could lead to unintended information disclosure, potentially allowing an attacker to gain unauthorized access to sensitive data.

[medium] CVE-2026-11979 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2, specifically within the xmlcatalog utility when operating in shell mode. An attacker can exploit multiple stack-based buffer overflows by providing an excessively long input line. This leads to memory corruption, which may cause the application to crash or potentially allow the attacker to execute arbitrary code within the context of the xmlcatalog process.

Fixed in: 0:2.9.13-14.el9_8.4

[medium] CVE-2026-12087 — perl-Socket@4:2.031

A flaw was found in the `perl-Socket` component. The `pack_ip_mreq_source()` function, which handles network socket operations, contains an out-of-bounds heap read vulnerability. An attacker providing a specially crafted input can cause the system to read beyond the intended memory buffer, potentially leading to information disclosure from adjacent memory regions.

[medium] CVE-2026-12610 — pam@1.5.1

A flaw was found in sssd. When authenticating with a YubiKey, the SSSD PAM responder can crash due to a use-after-free vulnerability, where a memory pointer is incorrectly handled. A local attacker could exploit this flaw by manipulating smartcard or YubiKey contents, leading to a denial of service that disrupts authentication. This vulnerability also presents a potential for privilege escalation, although it is difficult to exploit.

[medium] CVE-2026-13595 — libblkid@2.37.4-25.el9

A flaw was found in the libblkid library of util-linux. During nested partition probing, the BSD, Minix, Solaris x86, and UnixWare partition probers cache a raw pointer to a parent partition entry in a dynamically allocated array. When subsequent partition additions cause the array to be reallocated, this pointer becomes stale, leading to a heap use-after-free read. An attacker who can present a crafted block device image (for example, via USB insertion or a loop-mounted disk image) can trigger this flaw without user interaction, as libblkid is invoked automatically by udev/udisks as root on block-device hot-plug events. This could lead to limited information disclosure or denial of service.

[medium] CVE-2026-13595 — libmount@2.37.4-25.el9

A flaw was found in the libblkid library of util-linux. During nested partition probing, the BSD, Minix, Solaris x86, and UnixWare partition probers cache a raw pointer to a parent partition entry in a dynamically allocated array. When subsequent partition additions cause the array to be reallocated, this pointer becomes stale, leading to a heap use-after-free read. An attacker who can present a crafted block device image (for example, via USB insertion or a loop-mounted disk image) can trigger this flaw without user interaction, as libblkid is invoked automatically by udev/udisks as root on block-device hot-plug events. This could lead to limited information disclosure or denial of service.

[medium] CVE-2026-13595 — libsmartcols@2.37.4-25.el9

A flaw was found in the libblkid library of util-linux. During nested partition probing, the BSD, Minix, Solaris x86, and UnixWare partition probers cache a raw pointer to a parent partition entry in a dynamically allocated array. When subsequent partition additions cause the array to be reallocated, this pointer becomes stale, leading to a heap use-after-free read. An attacker who can present a crafted block device image (for example, via USB insertion or a loop-mounted disk image) can trigger this flaw without user interaction, as libblkid is invoked automatically by udev/udisks as root on block-device hot-plug events. This could lead to limited information disclosure or denial of service.

[medium] CVE-2026-13595 — libuuid@2.37.4-25.el9

A flaw was found in the libblkid library of util-linux. During nested partition probing, the BSD, Minix,

Solaris x86, and UnixWare partition probers cache a raw pointer to a parent partition entry in a dynamically allocated array. When subsequent partition additions cause the array to be reallocated, this pointer becomes stale, leading to a heap use-after-free read. An attacker who can present a crafted block device image (for example, via USB insertion or a loop-mounted disk image) can trigger this flaw without user interaction, as libblkid is invoked automatically by udev/udisks as root on block-device hot-plug events. This could lead to limited information disclosure or denial of service.

[medium] CVE-2026-13595 — util-linux@2.37.4

A flaw was found in the libblkid library of util-linux. During nested partition probing, the BSD, Minix, Solaris x86, and UnixWare partition probers cache a raw pointer to a parent partition entry in a dynamically allocated array. When subsequent partition additions cause the array to be reallocated, this pointer becomes stale, leading to a heap use-after-free read. An attacker who can present a crafted block device image (for example, via USB insertion or a loop-mounted disk image) can trigger this flaw without user interaction, as libblkid is invoked automatically by udev/udisks as root on block-device hot-plug events. This could lead to limited information disclosure or denial of service.

[medium] CVE-2026-1484 — glib2@2.68.4-19.el9_8.2

A flaw was found in the GLib Base64 encoding routine when processing very large input data. Due to incorrect use of integer types during length calculation, the library may miscalculate buffer boundaries. This can cause memory writes outside the allocated buffer. Applications that process untrusted or extremely large Base64 input using GLib may crash or behave unpredictably.

[medium] CVE-2026-1489 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. An integer overflow vulnerability in its Unicode case conversion implementation can lead to memory corruption. By processing specially crafted and extremely large Unicode strings, an attacker could trigger an undersized memory allocation, resulting in out-of-bounds writes. This could cause applications utilizing GLib for string conversion to crash or become unstable.

[medium] CVE-2026-15028 — libarchive@3.5.3-11.el9_8

A flaw was found in libarchive. This vulnerability allows a remote attacker to trigger a heap overflow by providing a specially crafted tar archive. The issue occurs during the parsing of a PAX extended header containing a malformed SUN.holesdata sparse-file attribute. Successful exploitation could lead to a denial of service, making the system unavailable, or potentially allow for arbitrary code execution, giving the attacker control over the affected system.

[medium] CVE-2026-15059 — systemd-libs@252-67.el9_8.4

A flaw was found in systemd-oomd. Local unprivileged users can exploit a missing path traversal validation in the systemd-oomd Inter-Process Communication (IPC) Application Programming Interface (API). This vulnerability allows them to terminate arbitrary local processes, leading to a denial of service.

[medium] CVE-2026-15588 — glib2@2.68.4-19.el9_8.2

A denial-of-service and resource exhaustion vulnerability exists within the `GDBus` component of GLib. The `gdbusauth` authentication mechanism fails to enforce proper length limitations on data lines read from a client. An unauthenticated local or remote attacker can exploit this lack of input validation by sending excessively long streams of data, causing the application to consume massive amounts of system memory and CPU, potentially leading to a crash or system hang.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-16118 — glib2@2.68.4-19.el9_8.2

A flaw was found in xdgmime. A heap-based buffer overflow can be triggered in _xdg_mime_magic_parse_magic_line() in the xdgmimemagic.c file on little-endian systems when an

attacker-controlled MIME magic file in a user-writable XDG data location (e.g., in the $XDG_DATA_HOME/mime/magic path) is parsed by an application performing MIME type detection (e.g., via g_content_type_guess()). When performing byte-swap, incorrect pointer arithmetic on the write side causes an out-of-bounds write of 2 bytes, resulting in an application crash or memory corruption.

Fixed in: 0:2.68.4-19.el9_8.10

[medium] CVE-2026-1757 — libxml2@2.9.13-14.el9_8.2

A flaw was identified in the interactive shell of the xmllint utility, part of the libxml2 project, where memory allocated for user input is not properly released under certain conditions. When a user submits input consisting only of whitespace, the program skips command execution but fails to free the allocated buffer. Repeating this action causes memory to continuously accumulate. Over time, this can exhaust system memory and terminate the xmllint process, creating a denial-of-service condition on the local system.

[medium] CVE-2026-18374 — glibc@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc). This vulnerability could allow an attacker with local access to trigger a heap buffer overflow by manipulating how the `fopen` function handles certain input. This could lead to minor disruptions in system operations or limited access to sensitive information.

[medium] CVE-2026-18374 — glibc@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc). This vulnerability could allow an attacker with local access to trigger a heap buffer overflow by manipulating how the `fopen` function handles certain input. This could lead to minor disruptions in system operations or limited access to sensitive information.

[medium] CVE-2026-18374 — glibc-common@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc). This vulnerability could allow an attacker with local access to trigger a heap buffer overflow by manipulating how the `fopen` function handles certain input. This could lead to minor disruptions in system operations or limited access to sensitive information.

[medium] CVE-2026-18374 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc). This vulnerability could allow an attacker with local access to trigger a heap buffer overflow by manipulating how the `fopen` function handles certain input. This could lead to minor disruptions in system operations or limited access to sensitive information.

[medium] CVE-2026-18477 — tar@2:1.34

A TOCTOU (Time-of-Check Time-of-Use) vulnerability in GNU tar's incremental dumpdir 'X' rename handling allows a local attacker with write access to a directory being backed up to influence the restore process if the attacker has access to the system where the restore is being performed. During restoration, files or directories may be created, renamed or overwritten outside the intended extraction directory. This could lead to unauthorized file modification or, in some cases, privilege escalation. Exploitation does not require the attacker to modify or craft the archive, and standard backup and restore workflows—including extracting into a newly created directory without using the -P option do not mitigate the issue.

Fixed in: 2:1.34-13.el9_8

[medium] CVE-2026-18508 — tar@2:1.34

A flaw was found in GNU tar. When extracting an archive with the --one-top-level option, hardlink targets are not confined to the designated top-level directory and may resolve relative to the extraction working directory. A crafted archive can create hardlinks that escape the intended boundary and, when combined with a preexisting symbolic link under the working directory, may allow writing outside that boundary during a single extraction.

Fixed in: 2:1.34-13.el9_8

[medium] CVE-2026-18798 — openssl@1:3.5.5

A flaw was found in OpenSSL. A malformed INITIAL packet with an invalid DCID (destination connection ID) can cause the QUIC server to double free the QRX object. This issue leads to memory corruption, causing the termination of the QUIC server process and resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[medium] CVE-2026-18798 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. A malformed INITIAL packet with an invalid DCID (destination connection ID) can cause the QUIC server to double free the QRX object. This issue leads to memory corruption, causing the termination of the QUIC server process and resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[medium] CVE-2026-19542 — glibc@2.34-275.el9_8

A flaw was found in glibc. An out-of-bounds array write vulnerability exists within the `tdelete` function. This issue occurs due to incorrect management of array sizes, which can lead to memory corruption. A local attacker with low privileges could potentially exploit this to cause a denial of service or disclose sensitive information.

[medium] CVE-2026-19542 — glibc@2.34-275.el9_8

A flaw was found in glibc. An out-of-bounds array write vulnerability exists within the `tdelete` function. This issue occurs due to incorrect management of array sizes, which can lead to memory corruption. A local attacker with low privileges could potentially exploit this to cause a denial of service or disclose sensitive information.

[medium] CVE-2026-19542 — glibc-common@2.34-275.el9_8

A flaw was found in glibc. An out-of-bounds array write vulnerability exists within the `tdelete` function. This issue occurs due to incorrect management of array sizes, which can lead to memory corruption. A local attacker with low privileges could potentially exploit this to cause a denial of service or disclose sensitive information.

[medium] CVE-2026-19542 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in glibc. An out-of-bounds array write vulnerability exists within the `tdelete` function. This issue occurs due to incorrect management of array sizes, which can lead to memory corruption. A local attacker with low privileges could potentially exploit this to cause a denial of service or disclose sensitive information.

[medium] CVE-2026-1965 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When an application uses libcurl to make multiple Negotiate-authenticated HTTP or HTTPS requests to the same server with different credentials, libcurl may incorrectly reuse an existing connection. This logical error can cause a subsequent request to be sent using the authentication of a previous user, leading to an authentication bypass.

Fixed in: 0:7.76.1-40.el9_8.5

[medium] CVE-2026-1965 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When an application uses libcurl to make multiple Negotiate-authenticated HTTP or HTTPS requests to the same server with different credentials, libcurl may incorrectly reuse an existing connection. This logical error can cause a subsequent request to be sent using the authentication of a previous user, leading to an authentication bypass.

Fixed in: 0:7.76.1-40.el9_8.5

[medium] CVE-2026-19931 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. This vulnerability allows an attacker to reuse an HTTP connection set up for a given hostname using Negotiate authentication. When an initial request is made with empty credentials, a subsequent user's request can be sent over a previously authenticated connection belonging to another user. This could lead to information disclosure or unauthorized access to sensitive data.

[medium] CVE-2026-19931 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. This vulnerability allows an attacker to reuse an HTTP connection set up for a given hostname using Negotiate authentication. When an initial request is made with empty credentials, a subsequent user's request can be sent over a previously authenticated connection belonging to another user. This could lead to information disclosure or unauthorized access to sensitive data.

[medium] CVE-2026-22185 — openldap@2.6.8-4.el9

A flaw was found in OpenLDAP Lightning Memory-Mapped Database (LMDB) mdb_load. When processing malformed input, a local attacker can exploit a heap buffer underflow vulnerability in the readline() function. This can lead to an out-of-bounds read, potentially causing a denial of service (DoS) and limited disclosure of heap memory contents.

[medium] CVE-2026-2673 — openssl@1:3.5.5

A key group selection preference flaw has been discovered in OpenSSL. An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key exchange group configuration includes the default by using the "DEFAULT" keyword. A less preferred key exchange may be used even when a more preferred group is supported by both client and server, if the group was not included among the client's initial predicated keyshares. This will sometimes be the case with the new hybrid post-quantum groups, if the client chooses to defer their use until specifically requested by the server. No OpenSSL FIPS modules are affected by this issue, the code in question lies outside the FIPS boundary.

[medium] CVE-2026-2673 — openssl-fips-provider@3.0.7-11.el9_8

A key group selection preference flaw has been discovered in OpenSSL. An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key exchange group configuration includes the default by using the "DEFAULT" keyword. A less preferred key exchange may be used even when a more preferred group is supported by both client and server, if the group was not included among the client's initial predicated keyshares. This will sometimes be the case with the new hybrid post-quantum groups, if the client chooses to defer their use until specifically requested by the server. No OpenSSL FIPS modules are affected by this issue, the code in question lies outside the FIPS boundary.

[medium] CVE-2026-2673 — openssl-fips-provider-so@3.0.7-11.el9_8

A key group selection preference flaw has been discovered in OpenSSL. An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key exchange group configuration includes the default by using the "DEFAULT" keyword. A less preferred key exchange may be used even when a more preferred group is supported by both client and server, if the group was not included among the client's initial predicated keyshares. This will sometimes be the case with the new hybrid post-quantum groups, if the client chooses to defer their use until specifically requested by the server. No OpenSSL FIPS modules are affected by this issue, the code in question lies outside the FIPS boundary.

[medium] CVE-2026-2673 — openssl-libs@1:3.5.5-6.el9_8

A key group selection preference flaw has been discovered in OpenSSL. An OpenSSL TLS 1.3 server may fail to negotiate the expected preferred key exchange group when its key exchange group

configuration includes the default by using the "DEFAULT" keyword. A less preferred key exchange may be used even when a more preferred group is supported by both client and server, if the group was not included among the client's initial predicated keyshares. This will sometimes be the case with the new hybrid post-quantum groups, if the client chooses to defer their use until specifically requested by the server. No OpenSSL FIPS modules are affected by this issue, the code in question lies outside the FIPS boundary.

[medium] CVE-2026-27456 — libblkid@2.37.4-25.el9

A flaw was found in util-linux. When an /etc/fstab entry is configured with the user,loop options, the `mount` program checks the file path with user permissions but later opens it with root privileges. This creates a brief Time-of-Check-Time-of-Use (TOCTOU) window where an attacker can substitute the intended file with a malicious symbolic link. This allows a local unprivileged user to mount any root-owned file or block device that contains a valid filesystem, gaining full read access to its contents.

[medium] CVE-2026-27456 — libmount@2.37.4-25.el9

A flaw was found in util-linux. When an /etc/fstab entry is configured with the user,loop options, the `mount` program checks the file path with user permissions but later opens it with root privileges. This creates a brief Time-of-Check-Time-of-Use (TOCTOU) window where an attacker can substitute the intended file with a malicious symbolic link. This allows a local unprivileged user to mount any root-owned file or block device that contains a valid filesystem, gaining full read access to its contents.

[medium] CVE-2026-27456 — libsmartcols@2.37.4-25.el9

A flaw was found in util-linux. When an /etc/fstab entry is configured with the user,loop options, the `mount` program checks the file path with user permissions but later opens it with root privileges. This creates a brief Time-of-Check-Time-of-Use (TOCTOU) window where an attacker can substitute the intended file with a malicious symbolic link. This allows a local unprivileged user to mount any root-owned file or block device that contains a valid filesystem, gaining full read access to its contents.

[medium] CVE-2026-27456 — libuuid@2.37.4-25.el9

A flaw was found in util-linux. When an /etc/fstab entry is configured with the user,loop options, the `mount` program checks the file path with user permissions but later opens it with root privileges. This creates a brief Time-of-Check-Time-of-Use (TOCTOU) window where an attacker can substitute the intended file with a malicious symbolic link. This allows a local unprivileged user to mount any root-owned file or block device that contains a valid filesystem, gaining full read access to its contents.

[medium] CVE-2026-27456 — util-linux@2.37.4

A flaw was found in util-linux. When an /etc/fstab entry is configured with the user,loop options, the `mount` program checks the file path with user permissions but later opens it with root privileges. This creates a brief Time-of-Check-Time-of-Use (TOCTOU) window where an attacker can substitute the intended file with a malicious symbolic link. This allows a local unprivileged user to mount any root-owned file or block device that contains a valid filesystem, gaining full read access to its contents.

[medium] CVE-2026-28390 — openssl@1:3.5.5

A flaw was found in OpenSSL. A remote attacker could exploit this vulnerability by sending a specially crafted Cryptographic Message Syntax (CMS) EnvelopedData message. During the processing of a KeyTransportRecipientInfo with RSA-OAEP encryption, the system attempts to access an optional parameter field without first verifying its presence. This leads to a NULL pointer dereference, which can cause applications processing the attacker-controlled CMS data to crash, resulting in a Denial of Service (DoS).

Fixed in: 1:3.5.5-3.el9_8

[medium] CVE-2026-31790 — openssl@1:3.5.5

A flaw was found in openssl. Applications that use RSASVE key encapsulation, a method for securely exchanging encryption keys, may inadvertently expose sensitive data. This vulnerability arises when an application processes a malicious, invalid RSA public key provided by an attacker without proper validation. Consequently, the application might send the contents of an uninitialized memory buffer, which could contain confidential information, to the attacker.

Fixed in: 1:3.5.5-2.el9_8

[medium] CVE-2026-32316 — jq@1.6

A flaw was found in jq, a command-line JSON processor. An attacker can exploit an integer overflow vulnerability by crafting queries that produce extremely large strings. This causes a 32-bit unsigned integer overflow in the buffer allocation size calculation, leading to a drastically undersized memory buffer. Subsequent memory copy operations then write the full string data into this undersized buffer, causing a heap-based buffer overflow. This can result in a Denial of Service (DoS) by crashing the process or potentially allow for further exploitation through heap corruption.

[medium] CVE-2026-32776 — expat@2.5.0

A flaw was found in libexpat. A remote attacker could exploit this vulnerability by providing specially crafted XML content with empty external parameter entities. This could lead to a NULL pointer dereference, causing the application to crash and resulting in a Denial of Service (DoS).

[medium] CVE-2026-32777 — expat@2.5.0

A flaw was found in libexpat. A remote attacker could exploit this vulnerability by providing specially crafted Document Type Definition (DTD) content. This could lead to an infinite loop during parsing, resulting in a Denial of Service (DoS) for the application using libexpat.

[medium] CVE-2026-32778 — expat@2.5.0

A flaw was found in libexpat. This vulnerability allows an attacker to trigger a NULL pointer dereference in the `setContext` function. This occurs when the system attempts to retry an operation after an out-of-memory condition, which can lead to a Denial of Service (DoS) for the affected application.

[medium] CVE-2026-33056 — tar@2:1.34

A flaw was found in tar-rs, a Rust library for reading and writing tar archives. When unpacking a crafted tar archive, an attacker can exploit a symbolic link vulnerability. By including a symlink followed by a directory with the same name, the library incorrectly applies file permissions to the symlink's target. This allows an attacker to modify the permissions of arbitrary directories outside the intended extraction location.

[medium] CVE-2026-33947 — jq@1.6

A flaw was found in jq, a command line JSON processor. Processing a crafted JSON document, specifically when a large array is used as a path argument to the `jv_setpath`, `jv_getpath` and `delpaths_sorted` functions can lead to an uncontrolled recursion and exhausts the call stack, causing an application crash and resulting in a denial of service.

[medium] CVE-2026-34182 — openssl@1:3.5.5

A flaw was found in OpenSSL's Cryptographic Message Services (CMS) AuthEnvelopedData processing. An on-path attacker can exploit insufficient input validation on cipher and tag length fields by sending specially crafted CMS messages. This can lead to the forging of messages or bypassing integrity validation. Consequently, an attacker may achieve key-equivalent functionality for a given CMS recipient.

Fixed in: 1:3.5.5-4.el9_8

[medium] CVE-2026-34183 — openssl@1:3.5.5

A flaw was found in OpenSSL's QUIC PATH_CHALLENGE handler. A remote attacker can exploit this vulnerability by flooding a QUIC client or server with specially crafted PATH_CHALLENGE frames. This leads to unbounded memory allocation within the local QUIC stack, as the system continuously allocates PATH_RESPONSE frames without them being acknowledged. The primary consequence is a Denial of Service (DoS), causing the affected application to terminate abnormally due to memory exhaustion.

Fixed in: 1:3.5.5-4.el9_8

[medium] CVE-2026-34743 — xz-libs@5.2.5-8.el9_0

A flaw was found in XZ Utils. When the `lzma_index_decoder()` function processes an empty index, and a subsequent `lzma_index_append()` operation is performed, insufficient memory is allocated. This can lead to a buffer overflow, potentially causing a denial of service (DoS) for affected systems.

[medium] CVE-2026-35414 — openssh@9.9p1

A flaw was found in OpenSSH. This vulnerability arises from the incorrect handling of the authorized_keys principals option in uncommon scenarios. Specifically, when a principals list is used with a Certificate Authority that includes comma characters, OpenSSH may misinterpret the input. This could lead to security bypasses, potentially allowing unintended access or information disclosure in specific authentication contexts.

Fixed in: 0:9.9p1-7.el9_8

[medium] CVE-2026-3783 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When an OAuth2 bearer token is used for an HTTP(S) transfer that redirects to a second URL, curl could unintentionally leak the token. This occurs if the second hostname has entries in the `.netrc` file, allowing the bearer token intended for the first host to be sent to the redirected host. This information disclosure could allow an attacker to gain unauthorized access.

Fixed in: 0:7.76.1-40.el9_8.5

[medium] CVE-2026-3783 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When an OAuth2 bearer token is used for an HTTP(S) transfer that redirects to a second URL, curl could unintentionally leak the token. This occurs if the second hostname has entries in the `.netrc` file, allowing the bearer token intended for the first host to be sent to the redirected host. This information disclosure could allow an attacker to gain unauthorized access.

Fixed in: 0:7.76.1-40.el9_8.5

[medium] CVE-2026-3784 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. This vulnerability allows curl to wrongly reuse an existing HTTP proxy connection when performing a CONNECT request to a server, even if the new request uses different authentication credentials for the HTTP proxy. This improper connection reuse could lead to an attacker gaining unauthorized access to resources or information intended for a different user.

[medium] CVE-2026-3784 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. This vulnerability allows curl to wrongly reuse an existing HTTP proxy connection when performing a CONNECT request to a server, even if the new request uses different authentication credentials for the HTTP proxy. This improper connection reuse could lead to an attacker gaining unauthorized access to resources or information intended for a different user.

[medium] CVE-2026-39956 — jq@1.6

A flaw was found in jq, a command line JSON processor. In release builds, the `_strindices` builtin function calls the `jv_string_indexes` function without checking that the arguments are actually strings. This missing validation allows an attacker who can supply non-string inputs to cause an application

crash and a limited memory read.

[medium] CVE-2026-40467 — gawk@5.1.0-6.el9

A flaw was found in gawk. A Use After Free vulnerability exists in the do_getline_redir() routine within the io.c program file. This vulnerability can be triggered by an attacker, potentially leading to a system crash and causing a Denial of Service (DoS).

[medium] CVE-2026-40468 — gawk@5.1.0-6.el9

A flaw was found in gawk. An integer overflow vulnerability could allow a local attacker to cause memory exhaustion, leading to a denial of service. This flaw may also enable an attacker to corrupt gawk's internal memory, potentially leading to system instability.

[medium] CVE-2026-40553 — gawk@5.1.0-6.el9

A flaw was found in gawk. A buffer overflow vulnerability exists in the `ftype()` routine, located in the `extension/readdir.c` program file. This vulnerability could allow an attacker to crash the program, resulting in a denial of service. It may also potentially lead to arbitrary code execution, though this has not been definitively confirmed.

[medium] CVE-2026-40612 — jq@1.6

A flaw was found in jq, a command line JSON processor. The `jv_contains` function does not have a depth limit when processing nested arrays or objects. This missing depth limit allows an attacker who can supply a sufficiently nested input structure to exhaust the stack memory, causing an application crash and resulting in a denial of service.

[medium] CVE-2026-4105 — systemd-libs@252-67.el9_8.4

A flaw was found in systemd. The systemd-machined service contains an Improper Access Control vulnerability due to insufficient validation of the class parameter in the RegisterMachine D-Bus (Desktop Bus) method. A local unprivileged user can exploit this by attempting to register a machine with a specific class value, which may leave behind a usable, attacker-controlled machine object. This allows the attacker to invoke methods on the privileged object, leading to the execution of arbitrary commands with root privileges on the host system.

[medium] CVE-2026-41256 — jq@1.6

A flaw was found in jq, a command line JSON processor. Top-level jq programs loaded from a file using the `-f` flag are truncated at the first embedded NUL byte. This issue allows an attacker who can supply a crafted filter file to prematurely truncate the program, potentially bypassing filtering logic and modifying the integrity of the processed data.

[medium] CVE-2026-41257 — jq@1.6

A flaw was found in jq, a command line JSON processor. The memory allocation size is calculated using a signed integer that can overflow when processing deeply nested generator forks. This integer overflow allows an attacker who can supply a sufficiently nested input to influence the memory allocation size, causing an out-of-bounds write and an application crash, resulting in a denial of service.

[medium] CVE-2026-41991 — gzip@1.12

A flaw was found in the `gzexe` utility of GNU `gzip`. When the `mktemp` utility is not available, `gzexe` creates temporary files with predictable names based on the process ID. A local attacker can exploit this by pre-creating a symbolic link to an arbitrary file at the predicted temporary file path. This can lead to a Time-of-Check to Time-of-Use (TOCTOU) condition, allowing the attacker to overwrite arbitrary files on the system.

Fixed in: 0:1.12-2.el9_8

[medium] CVE-2026-42250 — bzip2-libs@1.0.8-11.el9

A flaw was found in bzip2. The bzip2recover utility contains an off-by-one error that allows a local attacker to cause an out-of-bounds write to a global buffer by processing a specially crafted file. This memory corruption can lead to a crash, resulting in a Denial of Service (DoS).

[medium] CVE-2026-42764 — openssl@1:3.5.5

A flaw was found in the OpenSSL QUIC (Quick UDP Internet Connections) server. A remote attacker could send a specially crafted QUIC initial packet with an invalid token. If the server's address validation is explicitly disabled, this could lead to a NULL pointer dereference, causing the server process to terminate abnormally and resulting in a Denial of Service (DoS).

Fixed in: 1:3.5.5-4.el9_8

[medium] CVE-2026-43894 — jq@1.6

A flaw was found in jq, a tool used for processing JSON data from the command line. A remote attacker can exploit a vulnerability by providing a specially crafted large number as input. This can cause an internal calculation error, leading to a memory overflow where the attacker can write their own data into the system's memory, potentially resulting in the application crashing (Denial of Service).

[medium] CVE-2026-43895 — jq@1.6

A flaw was found in jq, a command line JSON processor. Embedded NUL bytes in import paths are truncated during module and data-file lookup, creating a mismatch between the intended import string and the actual file path opened. This issue allows an attacker who can supply a crafted script to access unintended files.

[medium] CVE-2026-43896 — jq@1.6

A flaw was found in jq, a command line JSON processor. The `jv_object_merge_recursive` function, reachable via the `*` operator when both operands are objects, does not have a depth limit when processing nested objects. This missing depth limit allows an attacker who can supply a sufficiently nested input structure to exhaust the stack memory, causing an application crash and resulting in a denial of service.

[medium] CVE-2026-4426 — libarchive@3.5.3-11.el9_8

A flaw was found in libarchive. An Undefined Behavior vulnerability exists in the zisofs decompression logic, caused by improper validation of a field (`pz_log2_bs`) read from ISO9660 Rock Ridge extensions. A remote attacker can exploit this by supplying a specially crafted ISO file. This can lead to incorrect memory allocation and potential application crashes, resulting in a denial-of-service (DoS) condition.

[medium] CVE-2026-44777 — jq@1.6

A flaw was found in jq, a command line JSON processor. The module loader fails to perform cycle detection when resolving imports. This missing cycle detection allows an attacker who can supply crafted modules with circular dependencies to exhaust the stack memory, causing an application crash, resulting in a denial of service.

[medium] CVE-2026-45445 — openssl@1:3.5.5

A flaw was found in OpenSSL. Applications that use the AES-OCB encryption method with a specific one-shot interface (EVP_Cipher()) will have their provided Initialization Vector (IV) silently discarded. This leads to the same internal cryptographic value being used repeatedly, which compromises the confidentiality of encrypted data. Additionally, this issue allows for the universal forgery of authentication tags, undermining the integrity of communications.

Fixed in: 1:3.5.5-4.el9_8

[medium] CVE-2026-47770 — jq@1.6

A flaw was found in jq, a command-line JSON processor. This vulnerability allows a local user or an attacker providing malicious input to cause a denial of service (DoS) by comparing two sufficiently deeply nested arrays using the '==' operator. This action exhausts the C stack due to uncontrolled recursion, leading to a crash of the jq process.

[medium] CVE-2026-4873 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. A remote attacker could exploit this by initiating an unencrypted connection (via IMAP, SMTP, or POP3) and then making a subsequent request to the same host that requires Transport Layer Security (TLS). Due to incorrect connection reuse, the subsequent request would bypass the TLS requirement, leading to the transmission of sensitive information in cleartext. This vulnerability, categorized as Cleartext Transmission of Sensitive Information (CWE-319), results in information disclosure.

[medium] CVE-2026-4873 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. A remote attacker could exploit this by initiating an unencrypted connection (via IMAP, SMTP, or POP3) and then making a subsequent request to the same host that requires Transport Layer Security (TLS). Due to incorrect connection reuse, the subsequent request would bypass the TLS requirement, leading to the transmission of sensitive information in cleartext. This vulnerability, categorized as Cleartext Transmission of Sensitive Information (CWE-319), results in information disclosure.

[medium] CVE-2026-49839 — jq@1.6

A flaw was found in jq, a command-line JSON processor. This vulnerability allows an attacker to trigger a heap out-of-bounds write by providing a specially crafted, oversized file to the `jq --rawfile` option. This can lead to a denial of service (DoS), making the affected system or application unavailable, and may also impact data integrity. Exploitation requires user interaction, as a user must process the malicious file.

[medium] CVE-2026-50219 — expat@2.5.0

A flaw was found in libexpat. This vulnerability occurs because the library, in versions before 2.8.2, does not properly track handler call depth when certain XML parsing functions are invoked from within handlers during a policy violation. This oversight can lead to a use-after-free condition, which may result in information disclosure, integrity loss, or denial of service.

Fixed in: 0:2.5.0-6.el9_8.3

[medium] CVE-2026-50812 — sqlite-libs@3.34.1-10.el9_8

A flaw was found in SQLite. The Session Extension in SQLite is vulnerable to a NULL pointer dereference. A remote attacker could exploit this by supplying a specially crafted, malformed changeset blob. This could lead to a denial of service, making the application unavailable to legitimate users.

[medium] CVE-2026-53655 — tar@2:1.34

A flaw was found in node-tar. This vulnerability arises because node-tar incorrectly applies PAX extended header size records to subsequent intermediary metadata headers, leading to a desynchronization of the tar stream cursor compared to other standard tar implementations. A remote attacker could exploit this by crafting a malicious archive, causing different interpretations of archive contents between node-tar and other tools. This could allow an attacker to hide malicious files or sensitive information from security scanners that rely on different tar parsing libraries, potentially leading to information disclosure or bypassing security controls.

[medium] CVE-2026-54371 — libattr@2.5.1-3.el9

A flaw was found in the `attr` package. This vulnerability allows a local attacker to perform a symlink traversal attack by replacing a pathname component with a symbolic link - either during directory

hierarchy traversal by `getfattr` or during backup restoration by `setfattr`, which reads and resolves full pathnames from backup files. In both cases, when these utilities are executed by a privileged process over a path controlled by the attacker, this can lead to local privilege escalation.

Fixed in: 0:2.6.0-1.el9_8

[medium] CVE-2026-54411 — pam@1.5.1

A flaw was found in Linux-PAM's `pam_userdb` module. This vulnerability, categorized as an Observable Timing Discrepancy (CWE-208), allows a local or network-adjacent attacker to recover plaintext passwords. By repeatedly attempting authentication and measuring response-timing differences during plaintext password comparison, an attacker can deduce the password. This flaw is exploitable when the `pam_userdb` module is configured to store and compare credentials in plaintext, which is not a default setting.

Fixed in: 0:1.5.1-27.el9_8.1

[medium] CVE-2026-54679 — jq@1.6

A flaw was found in jq, a command-line JSON processor. On 32-bit systems, a local attacker could exploit an integer overflow vulnerability in the `jvp_string_append` function. This could lead to a massive buffer overrun, resulting in a denial of service (DoS) condition.

[medium] CVE-2026-5545 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. An application using libcurl that performs an authenticated HTTP(S) request after a Negotiate-authenticated one to the same host may incorrectly reuse the previous connection. This authentication bypass vulnerability allows the second request to be sent over a connection authenticated with different credentials, potentially leading to unauthorized access or information disclosure.

[medium] CVE-2026-5545 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. An application using libcurl that performs an authenticated HTTP(S) request after a Negotiate-authenticated one to the same host may incorrectly reuse the previous connection. This authentication bypass vulnerability allows the second request to be sent over a connection authenticated with different credentials, potentially leading to unauthorized access or information disclosure.

[medium] CVE-2026-55653 — openssh@9.9p1

A flaw was found in OpenSSH. A malicious SSH server can exploit a double free vulnerability in the Diffie-Hellman Group Exchange (DH-GEX) client path. This occurs during FIPS (Federal Information Processing Standards) mode known-group validation when the client processes attacker-controlled DH-GEX group parameters. Successful exploitation leads to client-side process termination, resulting in a Denial of Service (DoS).

Fixed in: 0:9.9p1-9.el9_8

[medium] CVE-2026-55655 — openssh@9.9p1

A flaw was found in OpenSSH. A local unprivileged attacker on a Linux client host can hijack client-side X11 forwarding connections. This is possible by pre-binding the preferred abstract X socket name when X11 forwarding is enabled and a local UNIX-domain X socket is used. A successful attack can compromise the confidentiality of forwarded X11 traffic, including sensitive window contents and input, and may allow some manipulation of the forwarded session.

Fixed in: 0:9.9p1-9.el9_8

[medium] CVE-2026-56131 — expat@2.5.0

A use-after-free vulnerability in libexpat occurs because handler call depth isn't properly tracked when

XML_ResumeParser is invoked during policy violations. This flaw can lead to information disclosure, data corruption, or denial of service.

[medium] CVE-2026-56132 — expat@2.5.0

A flaw was found in libexpat, a library used for parsing XML data. An attacker could exploit a heap-based buffer overflow, a type of memory error, by providing specially crafted XML input. This vulnerability occurs when the library mishandles memory reallocation while processing XML, particularly when multiple parsers share data. Successful exploitation could allow the attacker to execute arbitrary code, access sensitive information, or cause the application to crash, leading to a denial of service.

Fixed in: 0:2.5.0-6.el9_8.3

[medium] CVE-2026-56391 — coreutils-single@8.32-41.el9_8

A flaw was found in GNU coreutils uniq. When processing specially crafted multibyte input with the --check-chars option, an attacker can trigger an out-of-bounds read. This vulnerability can lead to a denial of service (DoS) due to an application crash and potentially expose sensitive information from adjacent memory.

[medium] CVE-2026-56392 — coreutils-single@8.32-41.el9_8

A flaw was found in GNU coreutils, specifically in the `unexpand` utility. This vulnerability, a heap-based buffer overflow, occurs due to an integer overflow when `unexpand` processes unusually large tab stop values provided by a local attacker. This can lead to an undersized memory buffer, allowing subsequent operations to write beyond its boundaries. Successful exploitation can cause the `unexpand` utility to crash, potentially resulting in a denial of service or enabling further memory manipulation.

Fixed in: 0:8.32-41.el9_8.1

[medium] CVE-2026-56404 — expat@2.5.0

A flaw was found in libexpat. This vulnerability, an integer overflow in the `addBinding` function, could allow a local attacker to execute arbitrary code. By exploiting this, an attacker could gain control over the affected system, compromising its confidentiality and integrity.

[medium] CVE-2026-56405 — expat@2.5.0

A flaw was found in libexpat. An integer overflow vulnerability exists within the `getAttributeId` function. This flaw could allow an attacker to potentially disclose sensitive information or execute arbitrary code, leading to a compromise of the system's integrity and confidentiality.

[medium] CVE-2026-56406 — expat@2.5.0

A flaw was found in libexpat. An integer overflow vulnerability exists in the `XML_ParseBuffer` function due to a missing check. This flaw could allow an attacker to cause memory corruption, potentially leading to arbitrary code execution, information disclosure, or a denial of service.

[medium] CVE-2026-56407 — expat@2.5.0

An integer overflow exists in libexpat's doProlog function due to improper handling of entity value lengths. A local attacker could exploit this to execute arbitrary code or access sensitive system data.

[medium] CVE-2026-56412 — expat@2.5.0

A flaw was found in libexpat. This vulnerability, present in versions before 2.8.2, stems from improper handling of XML CDATA sections, where the library fails to adequately track the depth of handler calls. This can result in a 'use-after-free' error, a type of memory corruption that could allow an attacker to crash the application or potentially gain unauthorized control.

[medium] CVE-2026-5704 — tar@2:1.34

A flaw was found in tar. A remote attacker could exploit this vulnerability by crafting a malicious archive, leading to hidden file injection with fully attacker-controlled content. This bypasses pre-extraction inspection mechanisms, potentially allowing an attacker to introduce malicious files onto a system without detection.

Fixed in: 2:1.34-13.el9_8

[medium] CVE-2026-5745 — libarchive@3.5.3-11.el9_8

A flaw was found in libarchive. A NULL pointer dereference vulnerability exists in the ACL parsing logic, specifically within the archive_acl_from_text_nl() function. When processing a malformed ACL string (such as a bare "d" or "default" tag without subsequent fields), the function fails to perform adequate validation before advancing the pointer. An attacker can exploit this by providing a maliciously crafted archive, causing an application utilizing the libarchive API (such as bsdtar) to crash, resulting in a Denial of Service (DoS).

[medium] CVE-2026-5773 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. Due to a logical error in the connection reuse mechanism for SMB (Server Message Block) transfers, libcurl might reuse an existing SMB connection with a different share than intended. This vulnerability, categorized as CWE-488 (Exposure of Data Element to Wrong Session), could lead to the download of an incorrect file or the upload of a file to an unintended location when an application uses libcurl for SMB transfers.

[medium] CVE-2026-5773 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. Due to a logical error in the connection reuse mechanism for SMB (Server Message Block) transfers, libcurl might reuse an existing SMB connection with a different share than intended. This vulnerability, categorized as CWE-488 (Exposure of Data Element to Wrong Session), could lead to the download of an incorrect file or the upload of a file to an unintended location when an application uses libcurl for SMB transfers.

[medium] CVE-2026-58010 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. An off-by-one error can occur in the gvs_tuple_is_normal function in the glib/gvariant-serialiser.c file when doing an alignment padding check because the bounds check uses > instead of >=, causing an out-of-bounds read of only 1 byte. This issue can cause a minor information disclosure of 1 byte and a denial of service when the out-of-bounds read crosses a page boundary.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-58011 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. An out-of-bounds read of only 2 bytes can occur in the g_date_time_get_ymd function in the glib/gdatetime.c file when an invalid GDateTime object produced by the g_date_time_add_full function is processed. This flaw can corrupt the date output and potentially cause logic errors that may lead to a denial of service.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-58012 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. A buffer over-read can occur in the g_regex_replace function when used with the `G_REGEX_RAW` compile flag and case-change replacement escapes because the string_append function processes matched substrings using UTF-8 functions that assume valid UTF-8 input, even when the string is treated as raw bytes. This vulnerability can cause a minor information disclosure of 1-5 bytes and a denial of service when the buffer over-read crosses a page boundary.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-58013 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. A buffer over-read can occur in g_io_channel_read_line_backend() in the giochannel.c file when a custom line terminator with a length greater than one is set, causing memcmp to read past the GString buffer. This vulnerability can cause a minor information disclosure of 7 bytes or a denial of service when the buffer over-read crosses a page boundary.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-58014 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. An off-by-one error can occur in the g_key_file_get_locale_string_list function in the gkeyfile.c file when loading a key file with an empty value. This flaw can cause an out-of-bounds access of 1 byte or a denial of service when the out-of-bounds access crosses a page boundary.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-58015 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. The D-Bus client-side implementation of the DBUS_COOKIE_SHA1 SASL authentication mechanism does not validate the cookie_context parameter received from the server. A malicious D-Bus server can supply a cookie_context containing path traversal sequences, causing the client to read an arbitrary file and exfiltrate sensitive data by verifying guessed file contents against a generated hash.

Fixed in: 0:2.68.4-19.el9_8.9

[medium] CVE-2026-58055 — libnghttp2@1.43.0-6.el9_8.1

A flaw in nghttp2's nghttpx proxy allows a remote attacker to perform HTTP request smuggling and cross-client response-queue poisoning. This occurs because the proxy ambiguously forwards HTTP/1.1 Upgrade requests that contain a Content-Length header to reusable keep-alive backend connections.

Fixed in: 0:1.43.0-6.el9_8.2

[medium] CVE-2026-5958 — sed@4.8-10.el9

A Time-of-Check Time-of-Use (TOCTOU) race condition was found in GNU sed. When the -i (in-place) and --follow-symlinks options are used together, sed resolves the symlink but reopens the path for writing. An attacker with write access to the directory containing the symlink can swap it between the check and the open operations. If a privileged user executes sed in this manner on a path influenced by the attacker, it can lead to arbitrary file overwrites and potential privilege escalation.

[medium] CVE-2026-59871 — tar@2:1.34

A flaw was found in node-tar, a library for manipulating tar archives in Node.js. This vulnerability occurs when the library incorrectly converts specific archive path values into numbers, leading to an error during subsequent path processing. An attacker could exploit this to cause the application using node-tar to crash, resulting in a denial of service.

[medium] CVE-2026-59875 — tar@2:1.34

A flaw was found in node-tar, a library for manipulating tar archives in Node.js. A remote attacker could craft a malicious archive containing null characters (NUL bytes) in its metadata. When this archive is processed, the unstripped null characters can cause the application to terminate unexpectedly, leading to a Denial of Service (DoS).

[medium] CVE-2026-59995 — openssh@9.9p1

A flaw was found in OpenSSH. The `sftp` client, when used to download files from a malicious server with the 'sftp server:/path .' command, does not properly restrict where those files are saved. This allows an attacker to control the download location, potentially overwriting existing files or placing malicious files in sensitive directories on the client system, which could compromise system integrity.

Fixed in: 0:9.9p1-11.el9_8

[medium] CVE-2026-59996 — openssh@9.9p1

A flaw was found in OpenSSH, a widely used tool for secure remote access. When a user attempts to copy files between two different remote systems using the `scp` command, the file might be incorrectly placed in a directory above the intended destination. This unintended file placement could lead to data integrity issues or, in some cases, unauthorized access to sensitive information if files are stored in an exposed location.

Fixed in: 0:9.9p1-9.el9_8

[medium] CVE-2026-59997 — openssh@9.9p1

A flaw was found in OpenSSH. The internal-sftp component within sshd incorrectly processes command-line arguments, recognizing only the first nine. This limitation can prevent the application of intended security configurations for SFTP (SSH File Transfer Protocol) connections, potentially leading to a bypass of security properties.

[medium] CVE-2026-59998 — openssh@9.9p1

A flaw was found in OpenSSH. The sshd component has an undocumented security-relevant behavior where GSSAPIStrictAcceptorCheck has no value when the server is in a Windows Active Directory environment. This could lead to unintended information disclosure and impact data integrity.

[medium] CVE-2026-60000 — openssh@9.9p1

A flaw was found in OpenSSH's Secure Shell Daemon (sshd). This vulnerability allows a remote attacker to cause a denial of service by initiating an excessive number of authentication attempts. The issue arises from the mishandling of the MaxAuthTries setting specifically when using GSSAPIAuthentication, leading to resource exhaustion.

[medium] CVE-2026-60001 — openssh@9.9p1

A flaw was found in OpenSSH's SSH daemon (sshd). A remote attacker could exploit this vulnerability by repeatedly attempting authentication. The flaw allows the attacker to bypass the intended minimum authentication delay, which can facilitate brute-force attacks. This makes it easier for an attacker to guess valid credentials, potentially leading to unauthorized access or a denial of service.

[medium] CVE-2026-6253 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When curl is configured to use distinct proxies for different URL schemes, a redirect from a URL using an authenticated proxy to one using an unauthenticated proxy can inadvertently expose the initial proxy's credentials. This improper credential management (CWE-522) may allow an attacker to gain unauthorized access or information by intercepting these disclosed credentials.

[medium] CVE-2026-6253 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When curl is configured to use distinct proxies for different URL schemes, a redirect from a URL using an authenticated proxy to one using an unauthenticated proxy can inadvertently expose the initial proxy's credentials. This improper credential management (CWE-522) may allow an attacker to gain unauthorized access or information by intercepting these disclosed credentials.

[medium] CVE-2026-63072 — openssl@1:3.5.5

A flaw was found in OpenSSL. A crafted CMS (Cryptographic Message Syntax) message can cause an 8-byte out-of-bounds heap write when it is decrypted with CMS_decrypt(). This issue occurs because the CMS decryption process incorrectly sizes the key-unwrap output buffer when using the AES-WRAP-PAD unwrap primitive. This can lead to memory corruption, resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[medium] CVE-2026-63072 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. A crafted CMS (Cryptographic Message Syntax) message can cause an 8-byte out-of-bounds heap write when it is decrypted with CMS_decrypt(). This issue occurs because the CMS decryption process incorrectly sizes the key-unwrap output buffer when using the AES-WRAP-PAD unwrap primitive. This can lead to memory corruption, resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[medium] CVE-2026-63076 — openssl@1:3.5.5

A flaw was found in OpenSSL. A crafted CMP (Certificate Management Protocol) message can cause an invalid pointer dereference due to a missing type check in the password-based protection verification. A remote, unauthenticated attacker can crash applications acting as a CMP server or client, resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[medium] CVE-2026-63076 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. A crafted CMP (Certificate Management Protocol) message can cause an invalid pointer dereference due to a missing type check in the password-based protection verification. A remote, unauthenticated attacker can crash applications acting as a CMP server or client, resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[medium] CVE-2026-63379 — libevent@2.1.12-8.el9_4

A flaw was found in Libevent, an event notification library. An unauthenticated remote attacker can exploit a vulnerability where chunked HTTP (Hypertext Transfer Protocol) trailers are incorrectly merged into request headers. This allows the attacker to place security-sensitive fields in trailers, causing an upstream proxy and the Libevent application to interpret different effective headers. This can lead to header smuggling, authorization bypass, proxy-header spoofing, or cache poisoning.

Fixed in: 0:2.1.13-1.el9_8

[medium] CVE-2026-63381 — libevent@2.1.12-8.el9_4

A flaw was found in Libevent, an event notification library. A use-after-free vulnerability exists in the `evbuffer_add_buffer_reference` function when it processes an output buffer with a zero length. This can lead to a dangling pointer, which an attacker could exploit to cause memory corruption or crash the application.

Fixed in: 0:2.1.13-1.el9_8

[medium] CVE-2026-6368 — glibc@2.34-275.el9_8

A flaw was found in glibc (GNU C Library). A local attacker or application using the wordexp function with the WRDE_APPEND flag can trigger the interface to return invalid memory in the we_wordv member. This invalid memory, when subsequently processed by wordfree, may cause the process to abort, leading to a Denial of Service (DoS).

[medium] CVE-2026-6368 — glibc@2.34-275.el9_8

A flaw was found in glibc (GNU C Library). A local attacker or application using the wordexp function with the WRDE_APPEND flag can trigger the interface to return invalid memory in the we_wordv member. This invalid memory, when subsequently processed by wordfree, may cause the process to abort, leading to a Denial of Service (DoS).

[medium] CVE-2026-6368 — glibc-common@2.34-275.el9_8

A flaw was found in glibc (GNU C Library). A local attacker or application using the wordexp function

with the WRDE_APPEND flag can trigger the interface to return invalid memory in the we_wordv member. This invalid memory, when subsequently processed by wordfree, may cause the process to abort, leading to a Denial of Service (DoS).

[medium] CVE-2026-6368 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in glibc (GNU C Library). A local attacker or application using the wordexp function with the WRDE_APPEND flag can trigger the interface to return invalid memory in the we_wordv member. This invalid memory, when subsequently processed by wordfree, may cause the process to abort, leading to a Denial of Service (DoS).

[medium] CVE-2026-6390 — nano@5.6.1

A flaw was found in GNU nano's multi-buffer error message handling. When a user opens multiple files at startup and one triggers an ALERT-level error, a specially crafted filename containing printf format specifiers can be reinterpreted. This format string vulnerability may allow an attacker to achieve stack information disclosure, cause a denial of service (crash), or potentially perform arbitrary memory writes.

[medium] CVE-2026-6429 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When configured to use a .netrc file for credentials and follow HTTP redirects, libcurl can inadvertently send the password from the initial connection to the redirected host. This sensitive information disclosure occurs when both the original and redirect URLs use clear text HTTP, are performed over the same HTTP proxy, and the same connection is reused. This vulnerability, categorized as an Exposure of Sensitive Information to an Unauthorized Actor (CWE-200), could allow an attacker to obtain user credentials.

[medium] CVE-2026-6429 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When configured to use a .netrc file for credentials and follow HTTP redirects, libcurl can inadvertently send the password from the initial connection to the redirected host. This sensitive information disclosure occurs when both the original and redirect URLs use clear text HTTP, are performed over the same HTTP proxy, and the same connection is reused. This vulnerability, categorized as an Exposure of Sensitive Information to an Unauthorized Actor (CWE-200), could allow an attacker to obtain user credentials.

[medium] CVE-2026-6653 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2. A remote attacker can exploit a use-after-free vulnerability in the `xmlParseInternalSubset` function by providing maliciously crafted XML input. This improper handling of entity resolution can lead to a denial-of-service (DoS), making the affected system or application unavailable.

Fixed in: 0:2.9.13-14.el9_8.4

[medium] CVE-2026-6791 — glibc@2.34-275.el9_8

A flaw was found in glibc. When processing paths that start with a tilde (~) followed by a username, the `wordexp` function can be forced to allocate an excessive amount of memory on the program's stack. A remote attacker could exploit this by providing a very long username, leading to a stack exhaustion and causing a denial of service (DoS) for the affected application.

[medium] CVE-2026-6791 — glibc@2.34-275.el9_8

A flaw was found in glibc. When processing paths that start with a tilde (~) followed by a username, the `wordexp` function can be forced to allocate an excessive amount of memory on the program's stack. A remote attacker could exploit this by providing a very long username, leading to a stack exhaustion and causing a denial of service (DoS) for the affected application.

[medium] CVE-2026-6791 — glibc-common@2.34-275.el9_8

A flaw was found in glibc. When processing paths that start with a tilde (~) followed by a username, the `wordexp` function can be forced to allocate an excessive amount of memory on the program's stack. A remote attacker could exploit this by providing a very long username, leading to a stack exhaustion and causing a denial of service (DoS) for the affected application.

[medium] CVE-2026-6791 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in glibc. When processing paths that start with a tilde (~) followed by a username, the `wordexp` function can be forced to allocate an excessive amount of memory on the program's stack. A remote attacker could exploit this by providing a very long username, leading to a stack exhaustion and causing a denial of service (DoS) for the affected application.

[medium] CVE-2026-6843 — nano@5.6.1

A flaw was found in nano. A local user could exploit a format string vulnerability in the `statusline()` function. By creating a directory with a name containing `printf` specifiers, the application attempts to display this name, leading to a segmentation fault (SEGV). This results in a Denial of Service (DoS) for the `nano` application.

[medium] CVE-2026-7168 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When a user performs a transfer over an HTTP proxy using Digest authentication and then reuses the same handle for a second transfer with a different proxy host, libcurl incorrectly sends the `Proxy-Authorization` header intended for the first proxy to the second proxy. This could lead to the disclosure of sensitive authentication information to an unintended proxy, potentially allowing an attacker to gain unauthorized access or impersonate the user.

[medium] CVE-2026-7168 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When a user performs a transfer over an HTTP proxy using Digest authentication and then reuses the same handle for a second transfer with a different proxy host, libcurl incorrectly sends the `Proxy-Authorization` header intended for the first proxy to the second proxy. This could lead to the disclosure of sensitive authentication information to an unintended proxy, potentially allowing an attacker to gain unauthorized access or impersonate the user.

[medium] CVE-2026-73282 — openssh@9.9p1

A flaw was found in OpenSSH. A use-after-free vulnerability exists in the `ssh` client when handling concurrent remote-forwarding operations. This can occur if a remote forwarding is added via the local session multiplexing socket while a remote forwarding open request is pending with the server. A remote attacker with high attack complexity could potentially exploit this to achieve low impact on confidentiality and integrity.

Fixed in: 0:9.9p1-11.el9_8

[medium] CVE-2026-73283 — openssh@9.9p1

A flaw was found in OpenSSH's `sshd` component. The `restrict` keyword, designed to limit tunnel forwarding within the `authorized_keys` file, was not correctly enforced for tunnel forwarding. This issue could allow a local attacker to bypass intended security restrictions, potentially leading to unauthorized network access or resource usage through tunnels.

Fixed in: 0:9.9p1-11.el9_8

[medium] CVE-2026-76781 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2. A local user or an attacker providing a specially crafted XML catalog can trigger a NULL pointer dereference during XML catalog parsing. This occurs when a `nextCatalog` element lacks its mandatory `catalog` attribute, leading to the application crashing and causing a Denial of Service (DoS).

[medium] CVE-2026-76957 — expat@2.5.0

A flaw was found in libexpat. The library's handling of custom encoding callbacks lacks proper tracking of handler call depth, which can lead to a use-after-free vulnerability. This memory corruption flaw could allow a local attacker to cause a denial of service or potentially execute arbitrary code.

[medium] CVE-2026-78367 — rpm@4.16.1.3-40.el9

A vulnerability was found in RPM's rpmbuild tarball processing. When processing a crafted source archive, the getTarSpec() function in tools/rpmbuild.cc passes an attacker-controlled tar archive member name to rpmExpand() as part of a %{basename:...} macro expression. A specially crafted .spec member name can therefore inject RPM macros, including Lua expressions, resulting in arbitrary code execution with the privileges of the user running rpmbuild. This can be exploited when a victim or automated build system processes an attacker-controlled source tarball using rpmbuild tarball mode (such as -ts, -ta, or -tb).

[medium] CVE-2026-78367 — rpm-libs@4.16.1.3-40.el9

A vulnerability was found in RPM's rpmbuild tarball processing. When processing a crafted source archive, the getTarSpec() function in tools/rpmbuild.cc passes an attacker-controlled tar archive member name to rpmExpand() as part of a %{basename:...} macro expression. A specially crafted .spec member name can therefore inject RPM macros, including Lua expressions, resulting in arbitrary code execution with the privileges of the user running rpmbuild. This can be exploited when a victim or automated build system processes an attacker-controlled source tarball using rpmbuild tarball mode (such as -ts, -ta, or -tb).

[medium] CVE-2026-80489 — glibc@2.34-275.el9_8

A flaw was found in glibc. A remote attacker could exploit this vulnerability by providing specially crafted input during SHIFT_JISX0213 to UCS-4 text conversion. This crafted input can cause the application to repeatedly process a buffered character without consuming further input, leading to a persistent loop and a denial of service (DoS) condition. This could make the affected application unresponsive.

[medium] CVE-2026-80489 — glibc@2.34-275.el9_8

A flaw was found in glibc. A remote attacker could exploit this vulnerability by providing specially crafted input during SHIFT_JISX0213 to UCS-4 text conversion. This crafted input can cause the application to repeatedly process a buffered character without consuming further input, leading to a persistent loop and a denial of service (DoS) condition. This could make the affected application unresponsive.

[medium] CVE-2026-80489 — glibc-common@2.34-275.el9_8

A flaw was found in glibc. A remote attacker could exploit this vulnerability by providing specially crafted input during SHIFT_JISX0213 to UCS-4 text conversion. This crafted input can cause the application to repeatedly process a buffered character without consuming further input, leading to a persistent loop and a denial of service (DoS) condition. This could make the affected application unresponsive.

[medium] CVE-2026-80489 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in glibc. A remote attacker could exploit this vulnerability by providing specially crafted input during SHIFT_JISX0213 to UCS-4 text conversion. This crafted input can cause the application to repeatedly process a buffered character without consuming further input, leading to a persistent loop and a denial of service (DoS) condition. This could make the affected application unresponsive.

[medium] CVE-2026-82327 — libsolv@0.7.24-6.el9_8

A flaw was found in libsolv, a dependency-resolution library used by RPM-based package managers such as dnf and zypper to work with .solv repository cache files. When libsolv rewrites a .solv cache file, it reads directory-id values from the file's compressed filelist data without validating that they fall within the expected range. A corrupted or specially crafted .solv cache file (for example, one left in a torn state after an unclean system shutdown) can cause an out-of-bounds memory write when a tool such as dnf, yum, or zypper next processes it. Successful exploitation is expected to result in a crash of the affected tool (denial of service); it is not expected to allow arbitrary code execution because the out-of-bounds write always stores a fixed, non-attacker-controlled value.

[medium] CVE-2026-84837 — rpm@4.16.1.3-40.el9

A flaw was found in rpm. An attacker can exploit a command injection vulnerability by influencing the path or filename of a tarball processed by `rpmbuild -t*` to include shell metacharacters. This is particularly relevant in automated build or continuous integration (CI) workflows that ingest externally supplied artifact names. Successful exploitation allows for arbitrary command execution with the privileges of the build user, which could lead to information disclosure or disruption of the build environment.

[medium] CVE-2026-84837 — rpm-libs@4.16.1.3-40.el9

A flaw was found in rpm. An attacker can exploit a command injection vulnerability by influencing the path or filename of a tarball processed by `rpmbuild -t*` to include shell metacharacters. This is particularly relevant in automated build or continuous integration (CI) workflows that ingest externally supplied artifact names. Successful exploitation allows for arbitrary command execution with the privileges of the build user, which could lead to information disclosure or disruption of the build environment.

[medium] CVE-2026-86138 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2, a software library for parsing XML documents. An integer overflow within the `xmlDictAddQString` function can lead to a heap-based buffer overflow. This vulnerability could allow a local attacker to execute arbitrary code on the system, potentially compromising its integrity and confidentiality.

[medium] CVE-2026-86142 — libxml2@2.9.13-14.el9_8.2

A flaw in libxml2's xmlXPtrEvalXPtrPart function allows a local attacker to cause a heap-based buffer overflow. An integer overflow while processing an oversized xpointer() expression leads to incorrect memory allocation and an out-of-bounds write, potentially resulting in information disclosure, data corruption, or a denial of service (DoS).

[medium] CVE-2026-86143 — libxml2@2.9.13-14.el9_8.2

An integer overflow in the libxml2 xmlIO module occurs when data backlogs exceed maximum integer limits. This flaw passes negative length values to downstream write callbacks, creating an unsafe state that can lead to data corruption or compromise application confidentiality and integrity.

[medium] CVE-2026-86144 — libxml2@2.9.13-14.el9_8.2

A flaw in libxml2's XInclude processing (xmlXIncludeProcess and xmlXIncludeProcessTree) fails to propagate parser flags like XML_PARSE_NONET. This allows custom resource loaders to fetch external network resources, potentially enabling Server-Side Request Forgery (SSRF), XML External Entity (XXE) injection, or Denial of Service (DoS) attacks.

[medium] CVE-2026-86469 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib2. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION and creating the .goutputstream-XXXXXX temporary file fails, the library unlinks the destination and recreates it without exclusive creation or symlink protection. A

local attacker who can write to the destination directory can win that race and redirect the write to another file.

[medium] CVE-2026-8674 — glibc@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc) DNS stub resolver. This vulnerability allows a remote attacker on the local network to cause a denial of service by providing a specially crafted, excessively long search domain. When the resolver attempts to initialize with this long domain from /etc/resolv.conf or the LOCALDOMAIN environment variable, it triggers an assertion failure, which aborts the process. This can be exploited without privileges on the target system, potentially through network configuration mechanisms like DHCP or a VPN server.

[medium] CVE-2026-8674 — glibc@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc) DNS stub resolver. This vulnerability allows a remote attacker on the local network to cause a denial of service by providing a specially crafted, excessively long search domain. When the resolver attempts to initialize with this long domain from /etc/resolv.conf or the LOCALDOMAIN environment variable, it triggers an assertion failure, which aborts the process. This can be exploited without privileges on the target system, potentially through network configuration mechanisms like DHCP or a VPN server.

[medium] CVE-2026-8674 — glibc-common@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc) DNS stub resolver. This vulnerability allows a remote attacker on the local network to cause a denial of service by providing a specially crafted, excessively long search domain. When the resolver attempts to initialize with this long domain from /etc/resolv.conf or the LOCALDOMAIN environment variable, it triggers an assertion failure, which aborts the process. This can be exploited without privileges on the target system, potentially through network configuration mechanisms like DHCP or a VPN server.

[medium] CVE-2026-8674 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in the GNU C Library (glibc) DNS stub resolver. This vulnerability allows a remote attacker on the local network to cause a denial of service by providing a specially crafted, excessively long search domain. When the resolver attempts to initialize with this long domain from /etc/resolv.conf or the LOCALDOMAIN environment variable, it triggers an assertion failure, which aborts the process. This can be exploited without privileges on the target system, potentially through network configuration mechanisms like DHCP or a VPN server.

[medium] CVE-2026-89092 — glibc@2.34-275.el9_8

A flaw was found in glibc, specifically within the nscd service. A remote attacker, operating a malicious Domain Name System (DNS) server, could send an overly large DNS response. This could trigger a stack overflow in the nscd service, causing it to crash and leading to degraded DNS resolution for the system. There is also a remote possibility of nscd cache corruption.

[medium] CVE-2026-89092 — glibc@2.34-275.el9_8

A flaw was found in glibc, specifically within the nscd service. A remote attacker, operating a malicious Domain Name System (DNS) server, could send an overly large DNS response. This could trigger a stack overflow in the nscd service, causing it to crash and leading to degraded DNS resolution for the system. There is also a remote possibility of nscd cache corruption.

[medium] CVE-2026-89092 — glibc-common@2.34-275.el9_8

A flaw was found in glibc, specifically within the nscd service. A remote attacker, operating a malicious Domain Name System (DNS) server, could send an overly large DNS response. This could trigger a stack overflow in the nscd service, causing it to crash and leading to degraded DNS resolution for the system. There is also a remote possibility of nscd cache corruption.

[medium] CVE-2026-89092 — glibc-minimal-langpack@2.34-275.el9_8

A flaw was found in glibc, specifically within the nscd service. A remote attacker, operating a malicious Domain Name System (DNS) server, could send an overly large DNS response. This could trigger a stack overflow in the nscd service, causing it to crash and leading to degraded DNS resolution for the system. There is also a remote possibility of nscd cache corruption.

[medium] CVE-2026-89157 — pcre2@10.40-6.el9

A flaw was found in PCRE2. On 32-bit platforms, an attacker can provide a specially crafted large pattern, leading to an out-of-bounds write within the pcre2_pattern_convert function. This vulnerability can result in high integrity impact, such as data corruption, and potentially a low availability impact, causing a denial of service.

[medium] CVE-2026-89157 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2. On 32-bit platforms, an attacker can provide a specially crafted large pattern, leading to an out-of-bounds write within the pcre2_pattern_convert function. This vulnerability can result in high integrity impact, such as data corruption, and potentially a low availability impact, causing a denial of service.

[medium] CVE-2026-89158 — pcre2@10.40-6.el9

A flaw was found in PCRE2. On 32-bit platforms, an integer overflow in the `pcre2_compile_32` function can lead to an out-of-bounds write. This vulnerability could allow a remote attacker to achieve a high integrity impact and a low availability impact, potentially leading to data corruption or denial of service.

[medium] CVE-2026-89158 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2. On 32-bit platforms, an integer overflow in the `pcre2_compile_32` function can lead to an out-of-bounds write. This vulnerability could allow a remote attacker to achieve a high integrity impact and a low availability impact, potentially leading to data corruption or denial of service.

[medium] CVE-2026-8924 — curl-minimal@7.76.1-40.el9

A flaw was found in curl's cookie parsing logic. A malicious HTTP server can exploit this by setting 'super cookies' that bypass the Public Suffix List check. This allows an attacker-controlled origin to inject cookies that curl then transmits to unrelated third-party domains, leading to compromising request integrity.

[medium] CVE-2026-8924 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl's cookie parsing logic. A malicious HTTP server can exploit this by setting 'super cookies' that bypass the Public Suffix List check. This allows an attacker-controlled origin to inject cookies that curl then transmits to unrelated third-party domains, leading to compromising request integrity.

[medium] CVE-2026-8932 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. The libcurl library, used for transferring data with URLs, could improperly reuse existing network connections. This occurred even when changes to mutual Transport Layer Security (mTLS) settings, particularly those for client certificates, should have prevented such reuse. This issue could lead to a security feature bypass, where a client might use a connection with an unintended or weaker security configuration, potentially compromising the integrity or confidentiality of data.

[medium] CVE-2026-8932 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. The libcurl library, used for transferring data with URLs, could improperly reuse existing network connections. This occurred even when changes to mutual Transport Layer Security (mTLS) settings, particularly those for client certificates, should have prevented such reuse. This issue could lead to a security feature bypass, where a client might use a connection with an unintended or

weaker security configuration, potentially compromising the integrity or confidentiality of data.

[medium] CVE-2026-9149 — libsolv@0.7.24-6.el9_8

A flaw was found in libsolv. This heap buffer overflow vulnerability occurs when a victim processes a specially crafted `.solv` file containing negative size values in the `repo_add_solv` function. This leads to an undersized memory allocation and a subsequent out-of-bounds write. An attacker could exploit this to cause a denial of service (DoS).

[medium] CVE-2026-9150 — libsolv@0.7.24-6.el9_8

A flaw was found in libsolv. This stack-based buffer overflow vulnerability occurs in libsolv's Debian metadata parser when processing specially crafted Debian repository metadata. An attacker could exploit this by providing malicious SHA384 or SHA512 checksum tags, leading to memory corruption and a denial of service (DoS) in the affected system.

[medium] GHSA-265r-hfxg-fhmg (CVE-2024-40635) — github.com/containerd/containerd@v1.7.11

containerd has an integer overflow in User ID handling

Fixed in: 1.7.27

[medium] GHSA-273p-m2cw-6833 (CVE-2026-23831) — github.com/sigstore/rekor@v1.2.2

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

Fixed in: 1.5.0

[medium] GHSA-273p-m2cw-6833 (CVE-2026-23831) — github.com/sigstore/rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

Fixed in: 1.5.0

[medium] GHSA-273p-m2cw-6833 (CVE-2026-23831) — github.com/sigstore/rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

Fixed in: 1.5.0

[medium] GHSA-37cx-329c-33x3 (CVE-2026-25934) — github.com/go-git/go-git/v5@v5.11.0

go-git improperly verifies data integrity values for .idx and .pack files

Fixed in: 5.16.5

[medium] GHSA-37cx-329c-33x3 (CVE-2026-25934) — github.com/go-git/go-git/v5@v5.13.2

go-git improperly verifies data integrity values for .idx and .pack files

Fixed in: 5.16.5

[medium] GHSA-3xc5-wrhm-f963 (CVE-2026-41506) — github.com/go-git/go-git/v5@v5.11.0

go-git: Credential leak via cross-host redirect in smart HTTP transport

Fixed in: 5.18.0

[medium] GHSA-3xc5-wrhm-f963 (CVE-2026-41506) —

github.com/go-git/go-git/v5@v5.13.2

go-git: Credential leak via cross-host redirect in smart HTTP transport

Fixed in: 5.18.0

[medium] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

Fixed in: 0.52.0

[medium] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

Fixed in: 0.52.0

[medium] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

Fixed in: 0.52.0

[medium] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

Fixed in: 0.52.0

[medium] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

Fixed in: 0.52.0

[medium] GHSA-4c4x-jm2x-pf9j (CVE-2026-24117) — github.com/sigstore/rekor@v1.2.2

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

Fixed in: 1.5.0

[medium] GHSA-4c4x-jm2x-pf9j (CVE-2026-24117) — github.com/sigstore/rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

Fixed in: 1.5.0

[medium] GHSA-4c4x-jm2x-pf9j (CVE-2026-24117) — github.com/sigstore/rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

Fixed in: 1.5.0

[medium] GHSA-4v7x-pqxf-cx7m (CVE-2023-45288) — net/http

net/http, x/net/http2: close connections when receiving too many headers

Fixed in: 1.21.9

[medium] GHSA-59jp-pj84-45mr (CVE-2026-22772) — github.com/sigstore/fulcio@v1.4.3

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

Fixed in: 1.8.5

[medium] GHSA-59jp-pj84-45mr (CVE-2026-22772) — github.com/sigstore/fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

Fixed in: 1.8.5

[medium] GHSA-59jp-pj84-45mr (CVE-2026-22772) — github.com/sigstore/fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

Fixed in: 1.8.5

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.33.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.33.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.34.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.35.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.35.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.41.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — golang.org/x/net@v0.52.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[medium] GHSA-6f2p-296r-cc28 (CVE-2026-54168) — github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

Fixed in: 0.37.8

[medium] GHSA-6f2p-296r-cc28 (CVE-2026-54168) — github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

Fixed in: 0.37.8

[medium] GHSA-6f2p-296r-cc28 (CVE-2026-54168) — github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

Fixed in: 0.37.8

[medium] GHSA-6pjf-3r9x-m592 (CVE-2026-41888) — github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution's tag deletion bypasses `storage.delete.enabled` configuration

Fixed in: 3.1.1

[medium] GHSA-6wxm-mpqj-6jpf (CVE-2024-45339) — github.com/golang/glog@v1.2.2

Insecure Temporary File usage in github.com/golang/glog

Fixed in: 1.2.4

[medium] GHSA-7236-3392-c5c6 (CVE-2026-61711) — github.com/moby/buildkit@v0.12.5

BuildKit: Custom frontend could bypass Seccomp/AppArmor

Fixed in: 0.31.1

[medium] GHSA-7236-3392-c5c6 (CVE-2026-61711) — github.com/moby/buildkit@v0.16.0

BuildKit: Custom frontend could bypass Seccomp/AppArmor

Fixed in: 0.31.1

[medium] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

Fixed in: 0.52.0

[medium] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

Fixed in: 0.52.0

[medium] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

Fixed in: 0.52.0

[medium] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

Fixed in: 0.52.0

[medium] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

Fixed in: 0.52.0

[medium] GHSA-7jxh-36q5-gcqv (CVE-2026-53495) — github.com/containerd/containerd@v1.7.11

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service

Fixed in: 1.7.35

[medium] GHSA-7jxh-36q5-gcqv (CVE-2026-53495) —

github.com/containerd/containerd@v1.7.32

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service

Fixed in: 1.7.35

[medium] GHSA-846p-jg2w-w324 (CVE-2026-23991) — github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf affected by client DoS via malformed server response

Fixed in: 2.3.1

[medium] GHSA-846p-jg2w-w324 (CVE-2026-23991) — github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf affected by client DoS via malformed server response

Fixed in: 2.3.1

[medium] GHSA-9c54-x2g4-v92j (CVE-2026-49835) — github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality

[medium] GHSA-9c54-x2g4-v92j (CVE-2026-49835) — github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality

[medium] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

Fixed in: 0.52.0

[medium] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

Fixed in: 0.52.0

[medium] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

Fixed in: 0.52.0

[medium] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

Fixed in: 0.52.0

[medium] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

Fixed in: 0.52.0

[medium] GHSA-9vcr-p3rj-q5q6 (CVE-2026-49834) — github.com/sigstore/sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log

Fixed in: 1.2.0

[medium] GHSA-9vcr-p3rj-q5q6 (CVE-2026-49834) — github.com/sigstore/sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log

Fixed in: 1.2.0

[medium] GHSA-c6gw-w398-hv78 (CVE-2025-27144) — github.com/go-jose/go-jose/v3@v3.0.3

DoS in go-jose Parsing

Fixed in: 3.0.4

[medium] GHSA-c6gw-w398-hv78 (CVE-2025-27144) — github.com/go-jose/go-jose/v3@v3.0.3

DoS in go-jose Parsing

Fixed in: 3.0.4

[medium] GHSA-cp6g-7hqx-qxhp (CVE-2026-2303) — go.mongodb.org/mongo-driver@v1.14.0

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

Fixed in: 1.17.7

[medium] GHSA-cp6g-7hqx-qxhp (CVE-2026-2303) — go.mongodb.org/mongo-driver@v1.16.1

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

Fixed in: 1.17.7

[medium] GHSA-cp6g-7hqx-qxhp (CVE-2026-2303) — go.mongodb.org/mongo-driver@v1.16.1

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

Fixed in: 1.17.7

[medium] GHSA-crhj-59gh-8x96 (CVE-2026-45571) — github.com/go-git/go-git/v5@v5.11.0

go-git: Crafted repositories may modify main and submodule .git directories

Fixed in: 5.19.1

[medium] GHSA-crhj-59gh-8x96 (CVE-2026-45571) — github.com/go-git/go-git/v5@v5.13.2

go-git: Crafted repositories may modify main and submodule .git directories

Fixed in: 5.19.1

[medium] GHSA-cv4x-93xx-wgfj (CVE-2026-33022) — github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

Fixed in: 1.0.1

[medium] GHSA-cv4x-93xx-wgfj (CVE-2026-33022) — github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

Fixed in: 1.0.1

[medium] GHSA-cv4x-93xx-wgfj (CVE-2026-33022) —

github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

Fixed in: 1.0.1

[medium] GHSA-cv4x-93xx-wgfj (CVE-2026-33022) — github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

Fixed in: 1.0.1

[medium] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[medium] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[medium] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[medium] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[medium] GHSA-fcv2-xgw5-pqxf (CVE-2026-24137) — github.com/sigstore/sigstore@v1.8.15

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[medium] GHSA-fcv2-xgw5-pqxf (CVE-2026-24137) — github.com/sigstore/sigstore@v1.8.15

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[medium] GHSA-fcv2-xgw5-pqxf (CVE-2026-24137) — github.com/sigstore/sigstore@v1.8.2

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[medium] GHSA-fphv-w9fq-2525 (CVE-2026-23992) — github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf improperly validates the configured threshold for delegations

Fixed in: 2.3.1

[medium] GHSA-fphv-w9fq-2525 (CVE-2026-23992) — github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf improperly validates the configured threshold for delegations

Fixed in: 2.3.1

[medium] GHSA-gcjh-h69q-9w9g — github.com/google/cel-go@v0.23.2

cel-go: JSON Private Fields Exposed via NativeTypes and ParseStructTag

Fixed in: 0.29.0

[medium] GHSA-gcjh-h69q-9w9g — github.com/google/cel-go@v0.23.2

cel-go: JSON Private Fields Exposed via NativeTypes and ParseStructTag

Fixed in: 0.29.0

[medium] GHSA-h7vf-4x9w-h99v (CVE-2026-85732) — oras.land/oras-go/v2@v2.6.1

oras-go: Blind SSRF via unvalidated Link header URL in pagination allows internal network probing

Fixed in: 2.6.2

[medium] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[medium] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[medium] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[medium] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[medium] GHSA-jc7w-c686-c4v9 (CVE-2025-58058) — github.com/ulikunitz/xz@v0.5.11

github.com/ulikunitz/xz leaks memory when decoding a corrupted multiple LZMA archives

Fixed in: 0.5.15

[medium] GHSA-jfvp-7x6p-h2pv (CVE-2024-45310) — github.com/opencontainers/runc@v1.1.12

runc can be confused to create empty files/directories on the host

Fixed in: 1.1.14

[medium] GHSA-jhf3-xxhw-2wpp (CVE-2026-34165) — github.com/go-git/go-git/v5@v5.11.0

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

Fixed in: 5.17.1

[medium] GHSA-jhf3-xxhw-2wpp (CVE-2026-34165) — github.com/go-git/go-git/v5@v5.13.2

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

Fixed in: 5.17.1

[medium] GHSA-jpcc-p29g-p8mq (CVE-2026-47262) — github.com/containerd/containerd@v1.7.11

containerd image-triggered runtime DoS via unbounded group parsing

Fixed in: 1.7.33

[medium] GHSA-jpcc-p29g-p8mq (CVE-2026-47262) — github.com/containerd/containerd@v1.7.32

containerd image-triggered runtime DoS via unbounded group parsing

Fixed in: 1.7.33

[medium] GHSA-jqc5-w2xx-5vq4 (CVE-2026-24686) — github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf Path Traversal in TAP 4 Multirepo Client Allows Arbitrary File Write via Malicious Repository Names

Fixed in: 2.4.1

[medium] GHSA-jqc5-w2xx-5vq4 (CVE-2026-24686) — github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf Path Traversal in TAP 4 Multirepo Client Allows Arbitrary File Write via Malicious Repository Names

Fixed in: 2.4.1

[medium] GHSA-m3xc-h892-ggx6 (CVE-2026-44740) — github.com/go-git/go-billy/v5@v5.5.0

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

Fixed in: 5.9.0

[medium] GHSA-m3xc-h892-ggx6 (CVE-2026-44740) — github.com/go-git/go-billy/v5@v5.6.2

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

Fixed in: 5.9.0

[medium] GHSA-m6hq-p25p-ffr2 (CVE-2025-64329) — github.com/containerd/containerd@v1.7.11

containerd CRI server: Host memory exhaustion through Attach goroutine leak

Fixed in: 1.7.29

[medium] GHSA-pjcq-xvwq-hhpj (CVE-2026-32952) — github.com/Azure/go-ntlmssp@v0.0.0-20211209120228-48547f28849e

go-ntlmssp NTLM challenges can panic on malformed payloads

Fixed in: 0.1.1

[medium] GHSA-pmwq-pjrm-6p5r — github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior

Fixed in: 0.11.0

[medium] GHSA-pmwq-pjrm-6p5r — github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior

Fixed in: 0.11.0

[medium] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — github.com/docker/docker@v25.0.6+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — github.com/docker/docker@v27.4.1+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — github.com/docker/docker@v28.0.0+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — github.com/docker/docker@v28.0.0+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — google.golang.org/grpc@v1.67.1

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

Fixed in: 1.83.1

[medium] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — google.golang.org/grpc@v1.69.4

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

Fixed in: 1.83.1

[medium] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

Fixed in: 1.83.1

[medium] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

Fixed in: 1.83.1

[medium] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — google.golang.org/grpc@v1.79.3

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

Fixed in: 1.83.1

[medium] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — google.golang.org/grpc@v1.80.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

Fixed in: 1.83.1

[medium] GHSA-qgq7-7hm3-q39j (CVE-2026-71557) — github.com/go-git/go-git/v5@v5.11.0

go-git: Malicious reference names may modify files outside the reference storage

Fixed in: 5.19.2

[medium] GHSA-qgq7-7hm3-q39j (CVE-2026-71557) — github.com/go-git/go-git/v5@v5.13.2

go-git: Malicious reference names may modify files outside the reference storage

Fixed in: 5.19.2

[medium] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

Fixed in: 0.52.0

[medium] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

Fixed in: 0.52.0

[medium] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

Fixed in: 0.52.0

[medium] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

Fixed in: 0.52.0

[medium] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

Fixed in: 0.52.0

[medium] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — golang.org/x/net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — golang.org/x/net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — golang.org/x/net@v0.34.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — golang.org/x/net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — golang.org/x/net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] GHSA-rmx9-2pp3-xhcr (CVE-2026-25542) — github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

Fixed in: 1.0.2

[medium] GHSA-rmx9-2pp3-xhcr (CVE-2026-25542) — github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

Fixed in: 1.0.2

[medium] GHSA-rmx9-2pp3-xhcr (CVE-2026-25542) — github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

Fixed in: 1.0.2

[medium] GHSA-rmx9-2pp3-xhcr (CVE-2026-25542) — github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

Fixed in: 1.0.2

[medium] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — github.com/docker/docker@v25.0.6+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — github.com/docker/docker@v27.4.1+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — github.com/docker/docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — github.com/docker/docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] GHSA-vrw8-fxc6-2r93 — github.com/go-chi/chi/v5@v5.1.0

chi Allows Host Header Injection which Leads to Open Redirect in RedirectSlashes

Fixed in: 5.2.2

[medium] GHSA-vrw8-fxc6-2r93 — github.com/go-chi/chi/v5@v5.1.0

chi Allows Host Header Injection which Leads to Open Redirect in RedirectSlashes

Fixed in: 5.2.2

[medium] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — golang.org/x/net@v0.33.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[medium] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — golang.org/x/net@v0.33.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[medium] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — golang.org/x/net@v0.34.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[medium] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — golang.org/x/net@v0.35.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[medium] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — golang.org/x/net@v0.35.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[medium] GHSA-w5pp-99ch-qj29 — github.com/go-git/go-git/v5@v5.11.0

go-git: Malformed Git object data may cause panics or resource exhaustion

Fixed in: 5.19.1

[medium] GHSA-w5pp-99ch-qj29 — github.com/go-git/go-git/v5@v5.13.2

go-git: Malformed Git object data may cause panics or resource exhaustion

Fixed in: 5.19.1

[medium] GHSA-w67g-5rqw-f597 — github.com/gorilla/websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

Fixed in: 1.5.3

[medium] GHSA-w67g-5rqw-f597 — github.com/gorilla/websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

Fixed in: 1.5.3

[medium] GHSA-w67g-5rqw-f597 — github.com/gorilla/websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

Fixed in: 1.5.3

[medium] GHSA-w67g-5rqw-f597 — github.com/gorilla/websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

Fixed in: 1.5.3

[medium] GHSA-whqx-f9j3-ch6m (CVE-2026-22703) — github.com/sigstore/cosign/v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions

Fixed in: 2.6.2

[medium] GHSA-whqx-f9j3-ch6m (CVE-2026-22703) — github.com/sigstore/cosign/v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions

Fixed in: 2.6.2

[medium] GHSA-xjvp-4fhw-gc47 (CVE-2026-41579) — github.com/opencontainers/runc@v1.1.12

runc: Malicious image with /dev symlink can trigger limited host filesystem integrity violations

Fixed in: 1.3.6

[medium] GHSA-xmrv-pmrh-hhx2 — github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream@v1.6.8

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

Fixed in: 1.7.8

[medium] GHSA-xmrv-pmrh-hhx2 — github.com/aws/aws-sdk-go-v2/service/s3@v1.76.0

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

Fixed in: 1.97.3

[medium] GO-2025-3503 (CVE-2025-22870) — stdlib@go1.22.12

Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, when the NO_PROXY environment variable is set to "*.example.com", a request to "[::1%25.example.com]:80` will incorrectly match and not be proxied.

Fixed in: 1.23.7

[medium] GO-2025-3503 (CVE-2025-22870) — stdlib@go1.22.12

Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, when the NO_PROXY environment variable is set to "*.example.com", a request to "[::1%25.example.com]:80` will incorrectly match and not be proxied.

Fixed in: 1.23.7

[medium] GO-2025-3503 (CVE-2025-22870) — stdlib@go1.23.6

Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, when the NO_PROXY environment variable is set to "*.example.com", a request to "[::1%25.example.com]:80` will incorrectly match and not be proxied.

Fixed in: 1.23.7

[medium] GO-2025-3503 (CVE-2025-22870) — stdlib@go1.23.6

Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, when the NO_PROXY environment variable is set to "*.example.com", a request to "[::1%25.example.com]:80` will incorrectly match and not be proxied.

Fixed in: 1.23.7

[medium] GO-2025-3503 (CVE-2025-22870) — stdlib@go1.23.6

Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, when the NO_PROXY environment variable is set to "*.example.com", a request to "[::1%25.example.com]:80` will incorrectly match and not be proxied.

Fixed in: 1.23.7

[medium] GO-2025-3750 (CVE-2025-0913) — stdlib@go1.22.12

os.OpenFile(path, os.O_CREATE|O_EXCL) behaved differently on Unix and Windows systems when the target path was a dangling symlink. On Unix systems, OpenFile with O_CREATE and O_EXCL flags never follows symlinks. On Windows, when the target path was a symlink to a nonexistent location, OpenFile would create a file in that location. OpenFile now always returns an error when the O_CREATE and O_EXCL flags are both set and the target path is a symlink.

Fixed in: 1.23.10

[medium] GO-2025-3750 (CVE-2025-0913) — stdlib@go1.22.12

os.OpenFile(path, os.O_CREATE|O_EXCL) behaved differently on Unix and Windows systems when the target path was a dangling symlink. On Unix systems, OpenFile with O_CREATE and O_EXCL flags never follows symlinks. On Windows, when the target path was a symlink to a nonexistent location, OpenFile would create a file in that location. OpenFile now always returns an error when the O_CREATE and O_EXCL flags are both set and the target path is a symlink.

Fixed in: 1.23.10

[medium] GO-2025-3750 (CVE-2025-0913) — stdlib@go1.23.6

os.OpenFile(path, os.O_CREATE|O_EXCL) behaved differently on Unix and Windows systems when the target path was a dangling symlink. On Unix systems, OpenFile with O_CREATE and O_EXCL flags never follows symlinks. On Windows, when the target path was a symlink to a nonexistent location, OpenFile would create a file in that location. OpenFile now always returns an error when the O_CREATE and O_EXCL flags are both set and the target path is a symlink.

Fixed in: 1.23.10

[medium] GO-2025-3750 (CVE-2025-0913) — stdlib@go1.23.6

os.OpenFile(path, os.O_CREATE|O_EXCL) behaved differently on Unix and Windows systems when the target path was a dangling symlink. On Unix systems, OpenFile with O_CREATE and O_EXCL flags never follows symlinks. On Windows, when the target path was a symlink to a nonexistent location, OpenFile would create a file in that location. OpenFile now always returns an error when the O_CREATE and O_EXCL flags are both set and the target path is a symlink.

Fixed in: 1.23.10

[medium] GO-2025-3750 (CVE-2025-0913) — stdlib@go1.23.6

os.OpenFile(path, os.O_CREATE|O_EXCL) behaved differently on Unix and Windows systems when the target path was a dangling symlink. On Unix systems, OpenFile with O_CREATE and O_EXCL flags never follows symlinks. On Windows, when the target path was a symlink to a nonexistent location, OpenFile would create a file in that location. OpenFile now always returns an error when the O_CREATE and O_EXCL flags are both set and the target path is a symlink.

Fixed in: 1.23.10

[medium] GO-2025-3751 (CVE-2025-4673) — stdlib@go1.22.12

Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information.

Fixed in: 1.23.10

[medium] GO-2025-3751 (CVE-2025-4673) — stdlib@go1.22.12

Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information.

Fixed in: 1.23.10

[medium] GO-2025-3751 (CVE-2025-4673) — stdlib@go1.23.6

Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information.

Fixed in: 1.23.10

[medium] GO-2025-3751 (CVE-2025-4673) — stdlib@go1.23.6

Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information.

Fixed in: 1.23.10

[medium] GO-2025-3751 (CVE-2025-4673) — stdlib@go1.23.6

Proxy-Authorization and Proxy-Authenticate headers persisted on cross-origin redirects potentially leaking sensitive information.

Fixed in: 1.23.10

[medium] GO-2025-3956 (CVE-2025-47906) — stdlib@go1.22.12

If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.

Fixed in: 1.23.12

[medium] GO-2025-3956 (CVE-2025-47906) — stdlib@go1.22.12

If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.

Fixed in: 1.23.12

[medium] GO-2025-3956 (CVE-2025-47906) — stdlib@go1.23.6

If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.

Fixed in: 1.23.12

[medium] GO-2025-3956 (CVE-2025-47906) — stdlib@go1.23.6

If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.

Fixed in: 1.23.12

[medium] GO-2025-3956 (CVE-2025-47906) — stdlib@go1.23.6

If the PATH environment variable contains paths which are executables (rather than just directories), passing certain strings to LookPath ("", ".", and ".."), can result in the binaries listed in the PATH being unexpectedly returned.

Fixed in: 1.23.12

[medium] GO-2025-4008 (CVE-2025-58189) — stdlib@go1.22.12

When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.

Fixed in: 1.24.8

[medium] GO-2025-4008 (CVE-2025-58189) — stdlib@go1.22.12

When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.

Fixed in: 1.24.8

[medium] GO-2025-4008 (CVE-2025-58189) — stdlib@go1.23.6

When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.

Fixed in: 1.24.8

[medium] GO-2025-4008 (CVE-2025-58189) — stdlib@go1.23.6

When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.

Fixed in: 1.24.8

[medium] GO-2025-4008 (CVE-2025-58189) — stdlib@go1.23.6

When Conn.Handshake fails during ALPN negotiation the error contains attacker controlled information (the ALPN protocols sent by the client) which is not escaped.

Fixed in: 1.24.8

[medium] GO-2025-4010 (CVE-2025-47912) — stdlib@go1.22.12

The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.

Fixed in: 1.24.8

[medium] GO-2025-4010 (CVE-2025-47912) — stdlib@go1.22.12

The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.

Fixed in: 1.24.8

[medium] GO-2025-4010 (CVE-2025-47912) — stdlib@go1.23.6

The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.

Fixed in: 1.24.8

[medium] GO-2025-4010 (CVE-2025-47912) — stdlib@go1.23.6

The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.

Fixed in: 1.24.8

[medium] GO-2025-4010 (CVE-2025-47912) — stdlib@go1.23.6

The Parse function permits values other than IPv6 addresses to be included in square brackets within the host component of a URL. RFC 3986 permits IPv6 addresses to be included within the host component, enclosed within square brackets. For example: "http://[::1]/". IPv4 addresses and hostnames must not appear within square brackets. Parse did not enforce this requirement.

Fixed in: 1.24.8

[medium] GO-2025-4011 (CVE-2025-58185) — stdlib@go1.22.12

Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.

Fixed in: 1.24.8

[medium] GO-2025-4011 (CVE-2025-58185) — stdlib@go1.22.12

Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.

Fixed in: 1.24.8

[medium] GO-2025-4011 (CVE-2025-58185) — stdlib@go1.23.6

Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.

Fixed in: 1.24.8

[medium] GO-2025-4011 (CVE-2025-58185) — stdlib@go1.23.6

Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.

Fixed in: 1.24.8

[medium] GO-2025-4011 (CVE-2025-58185) — stdlib@go1.23.6

Parsing a maliciously crafted DER payload could allocate large amounts of memory, causing memory exhaustion.

Fixed in: 1.24.8

[medium] GO-2025-4012 (CVE-2025-58186) — stdlib@go1.22.12

Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.

Fixed in: 1.24.8

[medium] GO-2025-4012 (CVE-2025-58186) — stdlib@go1.22.12

Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.

Fixed in: 1.24.8

[medium] GO-2025-4012 (CVE-2025-58186) — stdlib@go1.23.6

Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.

Fixed in: 1.24.8

[medium] GO-2025-4012 (CVE-2025-58186) — stdlib@go1.23.6

Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.

Fixed in: 1.24.8

[medium] GO-2025-4012 (CVE-2025-58186) — stdlib@go1.23.6

Despite HTTP headers having a default limit of 1MB, the number of cookies that can be parsed does not have a limit. By sending a lot of very small cookies such as "a=;", an attacker can make an HTTP server allocate a large amount of structs, causing large memory consumption.

Fixed in: 1.24.8

[medium] GO-2025-4014 (CVE-2025-58183) — stdlib@go1.22.12

tar.Reader does not set a maximum size on the number of sparse region data blocks in GNU tar pax 1.0 sparse files. A maliciously-crafted archive containing a large number of sparse regions can cause a Reader to read an unbounded amount of data from the archive into memory. When reading from a compressed source, a small compressed input can result in large allocations.

Fixed in: 1.24.8

[medium] GO-2025-4014 (CVE-2025-58183) — stdlib@go1.22.12

tar.Reader does not set a maximum size on the number of sparse region data blocks in GNU tar pax 1.0 sparse files. A maliciously-crafted archive containing a large number of sparse regions can cause a Reader to read an unbounded amount of data from the archive into memory. When reading from a compressed source, a small compressed input can result in large allocations.

Fixed in: 1.24.8

[medium] GO-2025-4014 (CVE-2025-58183) — stdlib@go1.23.6

tar.Reader does not set a maximum size on the number of sparse region data blocks in GNU tar pax 1.0 sparse files. A maliciously-crafted archive containing a large number of sparse regions can cause a Reader to read an unbounded amount of data from the archive into memory. When reading from a compressed source, a small compressed input can result in large allocations.

Fixed in: 1.24.8

[medium] GO-2025-4014 (CVE-2025-58183) — stdlib@go1.23.6

tar.Reader does not set a maximum size on the number of sparse region data blocks in GNU tar pax 1.0 sparse files. A maliciously-crafted archive containing a large number of sparse regions can cause a Reader to read an unbounded amount of data from the archive into memory. When reading from a compressed source, a small compressed input can result in large allocations.

Fixed in: 1.24.8

[medium] GO-2025-4015 (CVE-2025-61724) — stdlib@go1.22.12

The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU

consumption.

Fixed in: 1.24.8

[medium] GO-2025-4015 (CVE-2025-61724) — stdlib@go1.22.12

The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[medium] GO-2025-4015 (CVE-2025-61724) — stdlib@go1.23.6

The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[medium] GO-2025-4015 (CVE-2025-61724) — stdlib@go1.23.6

The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[medium] GO-2025-4015 (CVE-2025-61724) — stdlib@go1.23.6

The Reader.ReadResponse function constructs a response string through repeated string concatenation of lines. When the number of lines in a response is large, this can cause excessive CPU consumption.

Fixed in: 1.24.8

[medium] GO-2025-4175 (CVE-2025-61727) — stdlib@go1.22.12

An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.

Fixed in: 1.24.11

[medium] GO-2025-4175 (CVE-2025-61727) — stdlib@go1.22.12

An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.

Fixed in: 1.24.11

[medium] GO-2025-4175 (CVE-2025-61727) — stdlib@go1.23.6

An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.

Fixed in: 1.24.11

[medium] GO-2025-4175 (CVE-2025-61727) — stdlib@go1.23.6

An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.

Fixed in: 1.24.11

[medium] GO-2025-4175 (CVE-2025-61727) — stdlib@go1.23.6

An excluded subdomain constraint in a certificate chain does not restrict the usage of wildcard SANs in the leaf certificate. For example a constraint that excludes the subdomain test.example.com does not prevent a leaf certificate from claiming the SAN *.example.com.

Fixed in: 1.24.11

[medium] GO-2026-4340 (CVE-2025-61730) — stdlib@go1.22.12

During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.

Fixed in: 1.24.12

[medium] GO-2026-4340 (CVE-2025-61730) — stdlib@go1.22.12

During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.

Fixed in: 1.24.12

[medium] GO-2026-4340 (CVE-2025-61730) — stdlib@go1.23.6

During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.

Fixed in: 1.24.12

[medium] GO-2026-4340 (CVE-2025-61730) — stdlib@go1.23.6

During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.

Fixed in: 1.24.12

[medium] GO-2026-4340 (CVE-2025-61730) — stdlib@go1.23.6

During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.

Fixed in: 1.24.12

[medium] GO-2026-4340 (CVE-2025-61730) — stdlib@go1.25.5

During the TLS 1.3 handshake if multiple messages are sent in records that span encryption level boundaries (for instance the Client Hello and Encrypted Extensions messages), the subsequent messages may be processed before the encryption level changes. This can cause some minor information disclosure if a network-local attacker can inject messages during the handshake.

Fixed in: 1.24.12

[medium] GO-2026-4342 (CVE-2025-61728) — stdlib@go1.22.12

archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an

archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.

Fixed in: 1.24.12

[medium] GO-2026-4342 (CVE-2025-61728) — stdlib@go1.22.12

archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.

Fixed in: 1.24.12

[medium] GO-2026-4342 (CVE-2025-61728) — stdlib@go1.23.6

archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.

Fixed in: 1.24.12

[medium] GO-2026-4342 (CVE-2025-61728) — stdlib@go1.23.6

archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.

Fixed in: 1.24.12

[medium] GO-2026-4342 (CVE-2025-61728) — stdlib@go1.23.6

archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.

Fixed in: 1.24.12

[medium] GO-2026-4342 (CVE-2025-61728) — stdlib@go1.25.5

archive/zip uses a super-linear file name indexing algorithm that is invoked the first time a file in an archive is opened. This can lead to a denial of service when consuming a maliciously constructed ZIP archive.

Fixed in: 1.24.12

[medium] GO-2026-4440 (CVE-2025-47911) — golang.org/x/net@v0.33.0

The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4440 (CVE-2025-47911) — golang.org/x/net@v0.33.0

The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4440 (CVE-2025-47911) — golang.org/x/net@v0.34.0

The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4440 (CVE-2025-47911) — golang.org/x/net@v0.35.0

The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4440 (CVE-2025-47911) — golang.org/x/net@v0.35.0

The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4440 (CVE-2025-47911) — golang.org/x/net@v0.41.0

The html.Parse function in golang.org/x/net/html has quadratic parsing complexity when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4441 (CVE-2025-58190) — golang.org/x/net@v0.33.0

The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4441 (CVE-2025-58190) — golang.org/x/net@v0.33.0

The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4441 (CVE-2025-58190) — golang.org/x/net@v0.34.0

The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4441 (CVE-2025-58190) — golang.org/x/net@v0.35.0

The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4441 (CVE-2025-58190) — golang.org/x/net@v0.35.0

The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4441 (CVE-2025-58190) — golang.org/x/net@v0.41.0

The html.Parse function in golang.org/x/net/html has an infinite parsing loop when processing certain inputs, which can lead to denial of service (DoS) if an attacker provides specially crafted HTML content.

Fixed in: 0.45.0

[medium] GO-2026-4603 (CVE-2026-27142) — stdlib@go1.22.12

Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.

Fixed in: 1.25.8

[medium] GO-2026-4603 (CVE-2026-27142) — stdlib@go1.22.12

Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.

Fixed in: 1.25.8

[medium] GO-2026-4603 (CVE-2026-27142) — stdlib@go1.23.6

Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.

Fixed in: 1.25.8

[medium] GO-2026-4603 (CVE-2026-27142) — stdlib@go1.23.6

Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.

Fixed in: 1.25.8

[medium] GO-2026-4603 (CVE-2026-27142) — stdlib@go1.23.6

Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.

Fixed in: 1.25.8

[medium] GO-2026-4603 (CVE-2026-27142) — stdlib@go1.25.5

Actions which insert URLs into the content attribute of HTML meta tags are not escaped. This can allow XSS if the meta tag also has an http-equiv attribute with the value "refresh". A new GODEBUG setting has been added, htmlmetacontenturlescape, which can be used to disable escaping URLs in actions in the meta content attribute which follow "url=" by setting htmlmetacontenturlescape=0.

Fixed in: 1.25.8

[medium] GO-2026-4864 (CVE-2026-32282) — stdlib@go1.22.12

On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.

Fixed in: 1.25.9

[medium] GO-2026-4864 (CVE-2026-32282) — stdlib@go1.22.12

On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.

Fixed in: 1.25.9

[medium] GO-2026-4864 (CVE-2026-32282) — stdlib@go1.23.6

On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.

Fixed in: 1.25.9

[medium] GO-2026-4864 (CVE-2026-32282) — stdlib@go1.23.6

On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.

Fixed in: 1.25.9

[medium] GO-2026-4864 (CVE-2026-32282) — stdlib@go1.23.6

On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.

Fixed in: 1.25.9

[medium] GO-2026-4864 (CVE-2026-32282) — stdlib@go1.25.5

On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can operate on the target of the symlink, even when the target lies outside the root. The Linux fchmodat syscall silently ignores the AT_SYMLINK_NOFOLLOW flag, which Root.Chmod uses to avoid symlink traversal. Root.Chmod checks its target before acting and returns an error if the target is a symlink lying outside the root, so the impact is limited to cases where the target is replaced with a symlink between the check and operation.

Fixed in: 1.25.9

[medium] GO-2026-4865 (CVE-2026-32289) — stdlib@go1.22.12

Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped,

leading to XSS vulnerabilities.

Fixed in: 1.25.9

[medium] GO-2026-4865 (CVE-2026-32289) — stdlib@go1.22.12

Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped, leading to XSS vulnerabilities.

Fixed in: 1.25.9

[medium] GO-2026-4865 (CVE-2026-32289) — stdlib@go1.23.6

Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped, leading to XSS vulnerabilities.

Fixed in: 1.25.9

[medium] GO-2026-4865 (CVE-2026-32289) — stdlib@go1.23.6

Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped, leading to XSS vulnerabilities.

Fixed in: 1.25.9

[medium] GO-2026-4865 (CVE-2026-32289) — stdlib@go1.23.6

Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped, leading to XSS vulnerabilities.

Fixed in: 1.25.9

[medium] GO-2026-4865 (CVE-2026-32289) — stdlib@go1.25.5

Context was not properly tracked across template branches for JS template literals, leading to possibly incorrect escaping of content when branches were used. Additionally template actions within JS template literals did not properly track the brace depth, leading to incorrect escaping being applied. These issues could cause actions within JS template literals to be incorrectly or improperly escaped, leading to XSS vulnerabilities.

Fixed in: 1.25.9

[medium] GO-2026-4869 (CVE-2026-32288) — stdlib@go1.22.12

tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive containing a large number of sparse regions encoded in the "old GNU sparse map" format.

Fixed in: 1.25.9

[medium] GO-2026-4869 (CVE-2026-32288) — stdlib@go1.22.12

tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive

containing a large number of sparse regions encoded in the "old GNU sparse map" format.

Fixed in: 1.25.9

[medium] GO-2026-4869 (CVE-2026-32288) — stdlib@go1.23.6

tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive containing a large number of sparse regions encoded in the "old GNU sparse map" format.

Fixed in: 1.25.9

[medium] GO-2026-4869 (CVE-2026-32288) — stdlib@go1.23.6

tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive containing a large number of sparse regions encoded in the "old GNU sparse map" format.

Fixed in: 1.25.9

[medium] GO-2026-4869 (CVE-2026-32288) — stdlib@go1.23.6

tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive containing a large number of sparse regions encoded in the "old GNU sparse map" format.

Fixed in: 1.25.9

[medium] GO-2026-4869 (CVE-2026-32288) — stdlib@go1.25.5

tar.Reader can allocate an unbounded amount of memory when reading a maliciously-crafted archive containing a large number of sparse regions encoded in the "old GNU sparse map" format.

Fixed in: 1.25.9

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.22.12

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.22.12

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.23.6

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by

GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.23.6

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.23.6

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.25.5

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.25.9

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4976 (CVE-2026-39825) — stdlib@go1.26.2

ReverseProxy can forward queries containing parameters not visible to Rewrite functions. When used with a Rewrite function, or a Director function which parses query parameters, ReverseProxy sanitizes the forwarded request to remove query parameters which are not parsed by url.ParseQuery. ReverseProxy does not take ParseQuery's limit on the total number of query parameters (controlled by GODEBUG=urlmaxqueryparams=N) into account. This can permit ReverseProxy to forward a request containing a query parameter that is not visible to the Rewrite function. For example, the query "a1=x&a2=x&...&a10000=x&hidden=y" can forward the parameter "hidden=y" while hiding it from the proxy's Rewrite function.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.22.12

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.22.12

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.23.6

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.23.6

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.23.6

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.25.5

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.25.9

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4980 (CVE-2026-39826) — stdlib@go1.26.2

If a trusted template author were to write a <script> tag containing an empty 'type' attribute or a 'type' attribute with an ASCII whitespace, the execution of the template would incorrectly escape any data passed into the <script> block.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.22.12

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.22.12

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.23.6

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.23.6

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.23.6

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.25.5

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.25.9

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-4982 (CVE-2026-39823) — stdlib@go1.26.2

CVE-2026-27142 fixed a vulnerability in which URLs were not correctly escaped inside of a <meta> tag's <content> attribute. If the URL content were to insert ASCII whitespaces around the '=' rune inside of the <content> attribute, the escaper would fail to similarly escape it, leading to XSS.

Fixed in: 1.25.10

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.34.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.41.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5025 (CVE-2026-42506) — golang.org/x/net@v0.52.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree.

This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.34.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.41.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5027 (CVE-2026-42502) — golang.org/x/net@v0.52.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.34.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.41.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5029 (CVE-2026-25681) — golang.org/x/net@v0.52.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.33.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.34.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.35.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.41.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5030 (CVE-2026-27136) — golang.org/x/net@v0.52.0

Parsing arbitrary HTML which is then rendered using Render can result in an unexpected HTML tree. This can be leveraged to execute XSS attacks in applications that attempt to sanitize input HTML before rendering.

Fixed in: 0.55.0

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.22.12

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.22.12

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.23.6

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.23.6

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.23.6

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.25.5

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.25.9

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5039 (CVE-2026-42507) — stdlib@go1.26.2

When returning errors, functions in the net/textproto package would include its input as part of the error. This might allow an attacker to inject misleading content to errors that are printed or logged.

Fixed in: 1.25.11

[medium] GO-2026-5158 (CVE-2026-41178) — go.opentelemetry.io/otel@v1.43.0

Opentelemetry-go's baggage parsing no longer caps raw header length in go.opentelemetry.io/otel

Fixed in: 1.42.0

[medium] GO-2026-5622 (CVE-2026-53489) — github.com/containerd/containerd@v1.7.11

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[medium] GO-2026-5622 (CVE-2026-53489) — github.com/containerd/containerd@v1.7.32

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[medium] GO-2026-5694 (CVE-2026-39395) — github.com/sigstore/cosign/v2@v2.4.3

Cosign's verify-blob-attestation reports false positive when payload parsing fails in github.com/sigstore/cosign

Fixed in: 2.6.3

[medium] GO-2026-5694 (CVE-2026-39395) — github.com/sigstore/cosign/v2@v2.4.3

Cosign's verify-blob-attestation reports false positive when payload parsing fails in github.com/sigstore/cosign

Fixed in: 2.6.3

[medium] GO-2026-5763 (CVE-2026-39984) — github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has Improper Certificate Validation in verifier in github.com/sigstore/timestamp-authority

[medium] GO-2026-5763 (CVE-2026-39984) — github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has Improper Certificate Validation in verifier in github.com/sigstore/timestamp-authority

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.22.12

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer

due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.22.12

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.23.6

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.23.6

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.23.6

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.25.5

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.25.9

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-5856 (CVE-2026-42505) — stdlib@go1.26.2

Handshakes which used Encrypted Client Hello could be de-anonymized by a passive network observer due to a disclosure of pre-shared key identities in the unencrypted client hello.

Fixed in: 1.25.12

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.22.12

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.22.12

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.23.6

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.23.6

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.23.6

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.25.5

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.25.9

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.26.2

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.26.5

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6091 (CVE-2026-56858) — stdlib@go1.26.5

Previously, pathological inputs could close an unescaped '/' early, allowing for attack-controlled data to inject arbitrary content, potentially leading to XSS.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.22.12

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.22.12

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for

'..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.23.6

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.23.6

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.23.6

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.25.5

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.25.9

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.26.2

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.26.5

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[medium] GO-2026-6218 (CVE-2026-56860) — stdlib@go1.26.5

Previously, resolving relative paths containing parent directory ('..') segments performed string conversions and buffer rewrites on each step, resulting in quadratic time complexity and high memory allocation overhead. Now, path resolution operates on a byte buffer using index-based backtracking for '..' segments, eliminating the quadratic time complexity and significantly reducing memory allocations.

Fixed in: 1.25.13

[low] CVE-2021-46195 — libgcc@11.5.0-14.el9

A flaw was discovered in the GNU libiberty library within the demangle_path() function in rust-demangle.c, as distributed in the GNU Compiler Collection (GCC). This flaw allows a crafted symbol to cause stack memory to be exhausted, leading to a crash.

[low] CVE-2021-46195 — libstdc++@11.5.0-14.el9

A flaw was discovered in the GNU libiberty library within the demangle_path() function in rust-demangle.c, as distributed in the GNU Compiler Collection (GCC). This flaw allows a crafted symbol to cause stack memory to be exhausted, leading to a crash.

[low] CVE-2022-27943 — libgcc@11.5.0-14.el9

A flaw was found in binutils, where GNU GCC is vulnerable to a denial of service caused by a stack consumption in the demangle_const() function in libiberty/rust-demangle.c. The vulnerability exists due to the application not properly controlling the consumption of internal resources. By persuading a victim to open a specially-crafted file, an attacker could cause a denial of service.

[low] CVE-2022-27943 — libstdc++@11.5.0-14.el9

A flaw was found in binutils, where GNU GCC is vulnerable to a denial of service caused by a stack consumption in the demangle_const() function in libiberty/rust-demangle.c. The vulnerability exists due to the application not properly controlling the consumption of internal resources. By persuading a victim to open a specially-crafted file, an attacker could cause a denial of service.

[low] CVE-2022-29458 — ncurses@6.2

A segmentation fault vulnerability was found in ncurses's convert_strings() function of tinfo/read_entry.c file. This flaw occurs due to corrupted terminfo data, triggering an out-of-bounds read error.

Fixed in: 0:6.2-10.20210508.el9_6.2

[low] CVE-2022-3219 — gnupg2@2.3.3-5.el9_7

A vulnerability was found in GnuPG. GnuPG can spin on a relatively small input by crafting a public key with thousands of signatures attached and compressed down to a few kilobytes. This issue can potentially cause a denial of service.

[low] CVE-2022-41409 — pcre2@10.40-6.el9

A flaw was found in PCRE2, where it is susceptible to an integer overflow vulnerability triggered by a negative repeat value in the pcre2test subject line that causes infinite looping. This flaw allows a remote attacker to pass specially crafted data to the application, initiating an integer overflow and executing a denial of service (DoS) attack.

[low] CVE-2022-41409 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2, where it is susceptible to an integer overflow vulnerability triggered by a negative repeat value in the pcre2test subject line that causes infinite looping. This flaw allows a remote attacker to pass specially crafted data to the application, initiating an integer overflow and

executing a denial of service (DoS) attack.

[low] CVE-2023-24056 — pkgconf@1.7.3

A flaw was found in pkgconf, where a variable duplication can cause unbounded string expansion due to incorrect checks in libpkgconf/tuple.c:pkgconf_tuple_parse. This issue may lead to a buffer overflow, which can crash the software.

[low] CVE-2023-32636 — glib2@2.68.4-19.el9_8.2

A flaw was found in glib, where the gvariant deserialization code is vulnerable to a denial of service introduced by additional input validation added to resolve CVE-2023-29499. The offset table validation may be very slow. This bug does not affect any released version of glib but does affect glib distributors who followed the guidance of glib developers to backport the initial fix for CVE-2023-29499.

[low] CVE-2023-39804 — tar@2:1.34

A flaw was found in tar. This issue occurs when extended attributes are processed in PAX archives, and could allow an attacker to cause an application crash, resulting in a denial of service.

[low] CVE-2023-4016 — procps-ng@3.3.17

A heap-based buffer overflow vulnerability was found in the procps project when handling untrusted input with the -C option. This issue may allow a user with "ps" utility access to write unfiltered data into the process heap, triggering an out-of-bounds write, consuming memory and causing a crash, resulting in a denial of service.

Fixed in: 0:3.3.17-13.el9

[low] CVE-2023-4156 — gawk@5.1.0-6.el9

A heap out-of-bounds read flaw was found in builtin.c in the gawk package. This issue may lead to a crash and could be used to read sensitive information.

[low] CVE-2023-45322 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2. In an out-of-memory condition or when limiting the memory allocation, processing a XML document using the HTML parser may result in a use-after-free vulnerability.

[low] CVE-2023-50495 — ncurses@6.2

A vulnerability was found in the NCurses package, where a segmentation fault may be triggered through _nc_wrap_entry().

[low] CVE-2023-50495 — ncurses-base@6.2-12.20210508.el9

A vulnerability was found in the NCurses package, where a segmentation fault may be triggered through _nc_wrap_entry().

[low] CVE-2023-50495 — ncurses-libs@6.2-12.20210508.el9

A vulnerability was found in the NCurses package, where a segmentation fault may be triggered through _nc_wrap_entry().

[low] CVE-2024-0232 — sqlite-libs@3.34.1-10.el9_8

A heap use-after-free issue has been identified in SQLite in the jsonParseAddNodeArray() function in sqlite3.c. This flaw allows a local attacker to leverage a victim to pass specially crafted malicious input to the application, potentially causing a crash and leading to a denial of service.

[low] CVE-2024-11053 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. A logic error when processing credentials from the .netrc file while performing redirects allows the transfer of credentials from the original host to the followed-to host under certain

circumstances, leaking the credentials to the followed-to host.

[low] CVE-2024-11053 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. A logic error when processing credentials from the .netrc file while performing redirects allows the transfer of credentials from the original host to the followed-to host under certain circumstances, leaking the credentials to the followed-to host.

[low] CVE-2024-13176 — openssl@1:3.5.5

A timing side-channel vulnerability was found in OpenSSL. This vulnerability allows an attacker to recover the private key. However, measuring the timing would require local access to the signing application or a fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This issue can happen with significant probability only for some of the supported elliptic curves. In particular, the NIST P-521 curve is affected.

[low] CVE-2024-13176 — openssl-libs@1:3.5.5-6.el9_8

A timing side-channel vulnerability was found in OpenSSL. This vulnerability allows an attacker to recover the private key. However, measuring the timing would require local access to the signing application or a fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This issue can happen with significant probability only for some of the supported elliptic curves. In particular, the NIST P-521 curve is affected.

[low] CVE-2024-41996 — openssl@1:3.5.5

A vulnerability was found in the Diffie-Hellman Ephemeral (DHE) Key Agreement Protocol, where a malicious client can exploit the server's public key validation process. By forcing the server to use DHE and validating the order of public keys, the client can trigger expensive server-side modular exponentiation calculations. This issue results in asymmetric resource consumption, potentially leading to a denial of service (DoS) attack by overwhelming the server with computationally intensive operations.

[low] CVE-2024-41996 — openssl-libs@1:3.5.5-6.el9_8

A vulnerability was found in the Diffie-Hellman Ephemeral (DHE) Key Agreement Protocol, where a malicious client can exploit the server's public key validation process. By forcing the server to use DHE and validating the order of public keys, the client can trigger expensive server-side modular exponentiation calculations. This issue results in asymmetric resource consumption, potentially leading to a denial of service (DoS) attack by overwhelming the server with computationally intensive operations.

[low] CVE-2024-5742 — nano@5.6.1

A vulnerability was found in GNU Nano that allows a possible privilege escalation through an insecure temporary file. If Nano is killed while editing, a file it saves to an emergency file with the permissions of the running user provides a window of opportunity for attackers to escalate privileges through a malicious symlink.

Fixed in: 0:5.6.1-6.el9

[low] CVE-2024-7264 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl, where libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If a syntactically incorrect field is given, the parser can use -1 for the length of the *time fraction*, leading to a `strlen()` performed on a pointer to a heap buffer area that is not purposely NULL terminated.

[low] CVE-2024-7264 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl, where libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If a syntactically incorrect field is given, the parser can use -1 for the length of the *time fraction*, leading to a `strlen()` performed on a pointer to a heap buffer area that is not purposely NULL terminated.

[low] CVE-2024-9681 — curl-minimal@7.76.1-40.el9

A vulnerability was found in curl. When curl is asked to use HSTS, the expiry time for a subdomain might overwrite a parent domain's cache entry, making it end sooner or later than intended.

[low] CVE-2024-9681 — libcurl-minimal@7.76.1-40.el9

A vulnerability was found in curl. When curl is asked to use HSTS, the expiry time for a subdomain might overwrite a parent domain's cache entry, making it end sooner or later than intended.

[low] CVE-2025-14524 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When an OAuth2 (Open Authorization) bearer token is used for an HTTP(S) transfer, and that transfer performs a cross-protocol redirect to a different scheme like IMAP, LDAP, POP3, or SMTP, curl might incorrectly pass the bearer token to the new target host. This could lead to information disclosure, where sensitive authentication tokens are exposed to unintended recipients.

[low] CVE-2025-14524 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When an OAuth2 (Open Authorization) bearer token is used for an HTTP(S) transfer, and that transfer performs a cross-protocol redirect to a different scheme like IMAP, LDAP, POP3, or SMTP, curl might incorrectly pass the bearer token to the new target host. This could lead to information disclosure, where sensitive authentication tokens are exposed to unintended recipients.

[low] CVE-2025-15079 — curl-minimal@7.76.1-40.el9

A flaw was found in curl. When performing SSH-based transfers using SCP or SFTP, libcurl could mistakenly connect to hosts not listed in the user-specified knownhosts file. This occurs if the host is present in the libssh global knownhosts file, effectively bypassing the intended host verification. This could allow a remote attacker to connect to an untrusted host, potentially leading to information disclosure or man-in-the-middle attacks.

[low] CVE-2025-15079 — libcurl-minimal@7.76.1-40.el9

A flaw was found in curl. When performing SSH-based transfers using SCP or SFTP, libcurl could mistakenly connect to hosts not listed in the user-specified knownhosts file. This occurs if the host is present in the libssh global knownhosts file, effectively bypassing the intended host verification. This could allow a remote attacker to connect to an untrusted host, potentially leading to information disclosure or man-in-the-middle attacks.

[low] CVE-2025-15224 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When doing SSH-based transfers using either SCP or SFTP, and asked to do public key authentication, curl would wrongly still ask and authenticate using a locally running SSH agent.

[low] CVE-2025-15224 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When doing SSH-based transfers using either SCP or SFTP, and asked to do public key authentication, curl would wrongly still ask and authenticate using a locally running SSH agent.

[low] CVE-2025-1632 — libarchive@3.5.3-11.el9_8

A flaw was found in the bsdunzip utility of libarchive. In affected versions, a specially crafted file may

trigger a null pointer dereference. This issue can lead to an application crash or other unexpected behavior. This bug does not compromise the integrity or availability of the base system.

[low] CVE-2025-27113 — libxml2@2.9.13-14.el9_8.2

A flaw was found in libxml2. This vulnerability allows a NULL pointer dereference, leading to a potential crash or denial of service via a crafted XML pattern.

[low] CVE-2025-30258 — gnupg2@2.3.3-5.el9_7

A flaw was found in GnuPG. In affected versions, if a user chooses to import a certificate with certain crafted subkey data that lacks a valid backsig or that has incorrect usage flags, the user loses the ability to verify signatures made from certain other signing keys, leading to a verification denial of service.

[low] CVE-2025-3360 — glib2@2.68.4-19.el9_8.2

A flaw was found in GLib. An integer overflow and buffer under-read occur when parsing a long invalid ISO 8601 timestamp with the g_date_time_new_from_iso8601() function.

[low] CVE-2025-5915 — libarchive@3.5.3-11.el9_8

A vulnerability has been identified in the libarchive library. This flaw can lead to a heap buffer over-read due to the size of a filter block potentially exceeding the Lempel-Ziv-Storer-Schieber (LZSS) window. This means the library may attempt to read beyond the allocated memory buffer, which can result in unpredictable program behavior, crashes (denial of service), or the disclosure of sensitive information from adjacent memory regions.

[low] CVE-2025-5916 — libarchive@3.5.3-11.el9_8

A vulnerability has been identified in the libarchive library. This flaw involves an integer overflow that can be triggered when processing a Web Archive (WARC) file that claims to have more than INT64_MAX - 4 content bytes. An attacker could craft a malicious WARC archive to induce this overflow, potentially leading to unpredictable program behavior, memory corruption, or a denial-of-service condition within applications that process such archives using libarchive. This bug affects libarchive versions prior to 3.8.0.

[low] CVE-2025-5917 — libarchive@3.5.3-11.el9_8

A vulnerability has been identified in the libarchive library. This flaw involves an 'off-by-one' miscalculation when handling prefixes and suffixes for file names. This can lead to a 1-byte write overflow. While seemingly small, such an overflow can corrupt adjacent memory, leading to unpredictable program behavior, crashes, or in specific circumstances, could be leveraged as a building block for more sophisticated exploitation. This bug affects libarchive versions prior to 3.8.0.

[low] CVE-2025-5918 — libarchive@3.5.3-11.el9_8

A vulnerability has been identified in the libarchive library. This flaw can be triggered when file streams are piped into bsdtar, potentially allowing for reading past the end of the file. This out-of-bounds read can lead to unintended consequences, including unpredictable program behavior, memory corruption, or a denial-of-service condition.

[low] CVE-2025-66382 — expat@2.5.0

A flaw was found in libexpat. This vulnerability allows a denial of service (DoS) by processing a crafted file with an approximate size of 2 MiB, leading to dozens of seconds of processing time.

[low] CVE-2025-7039 — glib2@2.68.4-19.el9_8.2

A flaw was found in glib. An integer overflow during temporary file creation leads to an out-of-bounds memory access, allowing an attacker to potentially perform path traversal or access private temporary file content by creating symbolic links. This vulnerability allows a local attacker to manipulate file paths

and access unauthorized data. The core issue stems from insufficient validation of file path lengths during temporary file operations.

[low] CVE-2025-70873 — sqlite-libs@3.34.1-10.el9_8

A flaw was found in SQLite. This information disclosure vulnerability exists within the zipfile extension, specifically in the zipfileInflate function. A remote attacker could exploit this by providing a specially crafted ZIP file. Successful exploitation could lead to the disclosure of sensitive heap memory information.

[low] CVE-2025-9232 — openssl@1:3.5.5

A flaw was found in the OpenSSL HTTP client API no_proxy handling. This vulnerability allows an application level denial of service (application crash) via an attacker-controlled IPv6 URL when the no_proxy environment variable is set.

[low] CVE-2025-9232 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in the OpenSSL HTTP client API no_proxy handling. This vulnerability allows an application level denial of service (application crash) via an attacker-controlled IPv6 URL when the no_proxy environment variable is set.

[low] CVE-2025-9403 — jq@1.6

A vulnerability has been identified in the jq JSON processor where malformed JSON input containing invalid Unicode escape sequences can trigger an assertion failure in the test suite’s parsing consistency checks. This flaw arises from inconsistencies between expected and reparsed JSON values during serialization and deserialization, potentially allowing an attacker to exploit the issue by supplying specially crafted JSON data to cause abnormal termination or denial of service during test execution, highlighting weaknesses in jq’s parsing reliability.

[low] CVE-2026-0988 — glib2@2.68.4-19.el9_8.2

A flaw was found in glib. Missing validation of offset and count parameters in the g_buffered_input_stream_peek() function can lead to an integer overflow during length calculation. When specially crafted values are provided, this overflow results in an incorrect size being passed to memcpy(), triggering a buffer overflow. This can cause application crashes, leading to a Denial of Service (DoS).

[low] CVE-2026-0989 — libxml2@2.9.13-14.el9_8.2

A flaw was identified in the RelaxNG parser of libxml2 related to how external schema inclusions are handled. The parser does not enforce a limit on inclusion depth when resolving nested <include> directives. Specially crafted or overly complex schemas can cause excessive recursion during parsing. This may lead to stack exhaustion and application crashes, creating a denial-of-service risk.

[low] CVE-2026-0992 — libxml2@2.9.13-14.el9_8.2

A flaw was found in the libxml2 library. This uncontrolled resource consumption vulnerability occurs when processing XML catalogs that contain repeated <nextCatalog> elements pointing to the same downstream catalog. A remote attacker can exploit this by supplying crafted catalogs, causing the parser to redundantly traverse catalog chains. This leads to excessive CPU consumption and degrades application availability, resulting in a denial-of-service condition.

[low] CVE-2026-14457 — openssl@1:3.5.5

A flaw was found in OpenSSL. In a server or client configuration with RFC7250 Raw Public Keys (RPKs) enabled, where only the private key (with no certificate) is configured, a NULL pointer dereference may occur when the remote peer solicits raw public keys and also sends the typically omitted "signature_algorithms_cert" TLS extension. This issue results in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-14457 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. In a server or client configuration with RFC7250 Raw Public Keys (RPKs) enabled, where only the private key (with no certificate) is configured, a NULL pointer dereference may occur when the remote peer solicits raw public keys and also sends the typically omitted "signature_algorithms_cert" TLS extension. This issue results in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-1485 — glib2@2.68.4-19.el9_8.2

A flaw was found in Glib's content type parsing logic. This buffer underflow vulnerability occurs because the length of a header line is stored in a signed integer, which can lead to integer wraparound for very large inputs. This results in pointer underflow and out-of-bounds memory access. Exploitation requires a local user to install or process a specially crafted treemagic file, which can lead to local denial of service or application instability.

[low] CVE-2026-18739 — popt@1.18-8.el9

A flaw was found in popt, a command-line option parsing library. An off-by-one error in the poptStuffArgs function, when repeatedly called by a host application or through deep alias nesting, can lead to corruption of internal program data. This corruption could potentially enable a local attacker to execute arbitrary code if the host application then unsafely processes the altered data.

[low] CVE-2026-18743 — popt@1.18-8.el9

A flaw was found in popt. This vulnerability allows an attacker to provide specially crafted configuration content to a host, which, when loaded, can lead to a small memory corruption issue. This occurs because of an error in how the `poptConfigFileToString` function reallocates memory for buffers. Successful exploitation could result in heap metadata corruption, potentially causing the affected process to become unavailable (denial of service).

[low] CVE-2026-18839 — popt@1.18-8.el9

An integer underflow was found in the popt library when formatting help text for option tables that exceed the terminal width. A local user who can cause an application to print help under those conditions may cause that application to crash or fail to display help, resulting in a denial of service of the affected application.

[low] CVE-2026-18924 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When libcurl handles HTTP/2 Server Push streams and the parent handle shares connections, a use-after-free vulnerability can occur during the cleanup process. This could lead to application crashes, resulting in a denial of service.

[low] CVE-2026-18924 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. When libcurl handles HTTP/2 Server Push streams and the parent handle shares connections, a use-after-free vulnerability can occur during the cleanup process. This could lead to application crashes, resulting in a denial of service.

[low] CVE-2026-24515 — expat@2.5.0

A null pointer dereference flaw has been discovered in libexpat. The function `XML_ExternalEntityParserCreate` failed to copy the encoding handler data passed to XML_SetUnknownEncodingHandler from the parent to the new subparser. This can cause a NULL dereference from external entities that declare use of an unknown encoding. The expected impact is denial of service. It takes use of both functions `XML_ExternalEntityParserCreate` and `XML_SetUnknownEncodingHandler` for an application to be vulnerable.

[low] CVE-2026-24883 — gnupg2@2.3.3-5.el9_7

A flaw was found in GnuPG. A remote attacker could provide a specially crafted long signature packet that, when processed, causes the application to crash. This vulnerability leads to a denial of service (DoS), making the GnuPG application unavailable to legitimate users.

[low] CVE-2026-27171 — zlib@1.2.11-40.el9

A flaw was found in zlib. An attacker providing specially crafted input to the `crc32_combine64` or `crc32_combine_gen64` functions could trigger an infinite loop within the `x2nmodp` function. This leads to excessive CPU consumption, which can result in a Denial of Service (DoS) for the affected system.

[low] CVE-2026-28387 — openssl@1:3.5.5

A flaw was found in OpenSSL. An uncommon configuration of clients performing DANE TLSA-based server authentication, when paired with uncommon server DANE TLSA records, may result in a use-after-free and/or double-free on the client side. This vulnerability could lead to data corruption, application crashes, or, in severe cases, arbitrary code execution. This issue is highly specific and uncommon, as it only affects clients using both PKIX-TA(0)/PKIX-EE(1) and DANE-TA(2) certificate usages and communicating with a server publishing a TLSA record set with both types of records.

[low] CVE-2026-28387 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. An uncommon configuration of clients performing DANE TLSA-based server authentication, when paired with uncommon server DANE TLSA records, may result in a use-after-free and/or double-free on the client side. This vulnerability could lead to data corruption, application crashes, or, in severe cases, arbitrary code execution. This issue is highly specific and uncommon, as it only affects clients using both PKIX-TA(0)/PKIX-EE(1) and DANE-TA(2) certificate usages and communicating with a server publishing a TLSA record set with both types of records.

[low] CVE-2026-28388 — openssl@1:3.5.5

A flaw was found in OpenSSL. When processing a malformed delta Certificate Revocation List (CRL) that lacks a required CRL Number extension, a NULL pointer dereference can occur. This vulnerability can be exploited by a remote attacker who provides a specially crafted delta CRL to an application that has delta CRL processing enabled, leading to a Denial of Service (DoS) for the application.

[low] CVE-2026-28388 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. When processing a malformed delta Certificate Revocation List (CRL) that lacks a required CRL Number extension, a NULL pointer dereference can occur. This vulnerability can be exploited by a remote attacker who provides a specially crafted delta CRL to an application that has delta CRL processing enabled, leading to a Denial of Service (DoS) for the application.

[low] CVE-2026-28389 — openssl@1:3.5.5

A flaw was found in OpenSSL. A remote attacker could exploit this by sending a specially crafted Cryptographic Message Syntax (CMS) EnvelopedData message with KeyAgreeRecipientInfo. This vulnerability arises because the software attempts to process an optional field without verifying its existence, leading to a NULL pointer dereference. This can result in a Denial of Service (DoS) for applications that handle untrusted CMS data.

[low] CVE-2026-28389 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. A remote attacker could exploit this by sending a specially crafted Cryptographic Message Syntax (CMS) EnvelopedData message with KeyAgreeRecipientInfo. This vulnerability arises because the software attempts to process an optional field without verifying its existence, leading to a NULL pointer dereference. This can result in a Denial of Service (DoS) for applications that handle untrusted CMS data.

[low] CVE-2026-31789 — openssl@1:3.5.5

A flaw was found in OpenSSL. This vulnerability, a heap buffer overflow, affects 32-bit systems when processing an unusually large X.509 certificate. If an application or service attempts to print or log such a specially crafted certificate, it could lead to a system crash or potentially allow an attacker to execute arbitrary code. This issue is considered low severity due to the specific conditions required for exploitation, including the need for an extremely large certificate and a 32-bit operating environment.

[low] CVE-2026-31789 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. This vulnerability, a heap buffer overflow, affects 32-bit systems when processing an unusually large X.509 certificate. If an application or service attempts to print or log such a specially crafted certificate, it could lead to a system crash or potentially allow an attacker to execute arbitrary code. This issue is considered low severity due to the specific conditions required for exploitation, including the need for an extremely large certificate and a 32-bit operating environment.

[low] CVE-2026-33948 — jq@1.6

A flaw was found in jq, a command-line JSON processor. This vulnerability allows a remote attacker to bypass input validation by crafting malicious JSON input containing embedded null (NUL) bytes. Due to incorrect handling of input buffer lengths, jq truncates the input at the first NUL byte, validating only the benign prefix and silently discarding any malicious data that follows. This can lead to parser differential attacks where downstream systems, relying on jq for validation, may process the full, unvalidated input, potentially leading to unexpected behavior or security compromises.

[low] CVE-2026-34180 — openssl@1:3.5.5

A flaw was found in OpenSSL. An integer truncation vulnerability in the ASN.1 decoder can occur when processing a crafted DER-encoded ASN.1 structure with a primitive element exceeding 2 gigabytes. A remote attacker could exploit this to cause a heap buffer over-read. This may lead to an application crash, resulting in a Denial of Service (DoS), or potentially disclose sensitive information by loading memory contents beyond the input buffer. This issue primarily affects 64-bit Unix and Unix-like platforms.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-34181 — openssl@1:3.5.5

A flaw was found in OpenSSL. This vulnerability allows a remote attacker to forge PKCS#12 (Public-Key Cryptography Standards #12) files that use Password-Based Message Authentication Code 1 (PBMAC1) with short HMAC (Hash-based Message Authentication Code) keys. This can lead to a service accepting attacker-controlled certificates and private keys with a 1 in 256 probability, potentially enabling impersonation.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-35386 — openssh@9.9p1

A flaw was found in OpenSSH. This vulnerability allows a remote attacker to achieve arbitrary command execution by injecting shell metacharacters into a username provided on the command line. Exploitation requires an untrusted username and a non-default configuration of the '%' character in `ssh_config`.

Fixed in: 0:9.9p1-7.el9_8

[low] CVE-2026-35387 — openssh@9.9p1

A flaw was found in OpenSSH. This vulnerability allows the system to use unintended Elliptic Curve Digital Signature Algorithm (ECDSA) algorithms. This occurs because the configuration for accepted public key algorithms is misinterpreted, leading to the use of weaker cryptographic methods than intended. This could potentially allow an attacker to compromise the confidentiality of data.

Fixed in: 0:9.9p1-7.el9_8

[low] CVE-2026-35388 — openssh@9.9p1

A flaw was found in OpenSSH. This vulnerability allows for a low integrity impact due to the omission of connection multiplexing confirmation for proxy-mode multiplexing sessions. A local user, under specific and complex conditions requiring user interaction, could potentially establish a multiplexed session without explicit confirmation, leading to unintended data handling.

Fixed in: 0:9.9p1-7.el9_8

[low] CVE-2026-41080 — expat@2.5.0

A flaw was found in libexpat. A remote attacker could exploit this vulnerability by providing a specially crafted XML document that leverages insufficient entropy in the hash function. This can lead to hash flooding, a type of Denial of Service (DoS) attack, where the system becomes unresponsive or crashes due to excessive resource consumption.

[low] CVE-2026-41990 — libgcrypt@1.10.0-13.el9_8

A flaw was found in Libgcrypt. During Dilithium signing operations, the library fails to perform a bounds check when writing to a static array. While the data involved is not directly controlled by an attacker, this vulnerability could lead to memory corruption, potentially resulting in a denial of service (DoS) or affecting data integrity.

[low] CVE-2026-41992 — gzip@1.12

A flaw was found in GNU gzip. This global buffer overflow vulnerability in the LZH decompression logic is caused by improper reuse of shared global state between different decompression formats. An attacker can exploit this by providing a specially crafted LZW file followed by a specially crafted LZH file to the `gzip -d` command. This can lead to an out-of-bounds read, potentially resulting in information disclosure.

Fixed in: 0:1.12-2.el9_8

[low] CVE-2026-42766 — openssl@1:3.5.5

A flaw was found in OpenSSL. A remote attacker could exploit a NULL pointer dereference vulnerability in the Cryptographic Message Syntax (CMS) decryption process by providing a specially crafted password-encrypted CMS message. This occurs because the keyDerivationAlgorithm field, which is optional, is dereferenced without proper validation. Successful exploitation leads to an application crash, resulting in a Denial of Service.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-42767 — openssl@1:3.5.5

A flaw was found in OpenSSL. An attacker controlling a Certificate Management Protocol (CMP) server, or acting as a man-in-the-middle, could craft a malicious CMP response. This response, containing a Certificate Request Message Format (CRMF) CertRepMessage with a specific malformed EncryptedValue structure, would trigger a NULL pointer dereference in the OpenSSL CMP client. This vulnerability leads to a crash of the application, resulting in a Denial of Service (DoS).

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-42768 — openssl@1:3.5.5

A flaw was found in OpenSSL's CMS_decrypt() and PKCS7_decrypt() functions. This vulnerability, a Bleichenbacher-style oracle, could allow a remote attacker to decrypt or sign messages using the victim's private RSA key. Exploitation requires the attacker to provide specially crafted CMS or S/MIME messages and observe the application's error codes or decryption output. While the attack is technically possible, the specific conditions required make it unlikely to be exploited in typical deployments.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-42769 — openssl@1:3.5.5

A flaw was found in the Certificate Management Protocol (CMP) implementation within OpenSSL. An attacker with existing Registration Authority (RA) level credentials could exploit an error in the certificate verification process during a Root Certificate Authority (CA) key update. This vulnerability allows the attacker to replace the root CA certificate for CMP clients with a fraudulent one. The primary consequence is an escalation of privileges, enabling the attacker to gain control equivalent to the root CA.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-42770 — openssl@1:3.5.5

A flaw was found in OpenSSL. A malicious peer can exploit this vulnerability by presenting a specially crafted DHX (X9.42) peer key. Due to improper validation of the peer key's subgroup membership, an attacker can recover the victim's private key after a small number of key exchange attempts. This information disclosure can lead to unauthorized access or further compromise of affected systems.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-44605 — rpm@4.16.1.3-40.el9

A flaw was found in the RPM Package Manager (RPM). A local user could be affected by a heap buffer overflow vulnerability when processing a specially crafted NDB database file. This issue arises from an error in how RPM handles certain calculations during file parsing, leading to an incorrect memory allocation. An attacker could leverage this to cause a denial of service, making the system unavailable.

[low] CVE-2026-44605 — rpm-libs@4.16.1.3-40.el9

A flaw was found in the RPM Package Manager (RPM). A local user could be affected by a heap buffer overflow vulnerability when processing a specially crafted NDB database file. This issue arises from an error in how RPM handles certain calculations during file parsing, leading to an incorrect memory allocation. An attacker could leverage this to cause a denial of service, making the system unavailable.

[low] CVE-2026-45446 — openssl@1:3.5.5

A flaw was found in OpenSSL. The implementations of AES-SIV (Advanced Encryption Standard - SIV) and AES-GCM-SIV (Advanced Encryption Standard - Galois/Counter Mode - SIV) incorrectly process authentication tags for empty messages. This vulnerability allows a remote attacker to forge empty messages with arbitrary Additional Authenticated Data (AAD) in applications that utilize these specific cipher modes within custom protocols and do not properly handle zero-length ciphertexts. This could lead to unauthorized data manipulation.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-54874 — openssl@1:3.5.5

A flaw was found in OpenSSL. Receiving a DTLS (Datagram Transport Layer Security) record for a future epoch while a handshake is in progress causes OpenSSL to buffer an excessive amount of memory. This allows a peer to cause memory exhaustion, eventually resulting in a denial of service, using a small amount of network traffic.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-54874 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. Receiving a DTLS (Datagram Transport Layer Security) record for a future epoch while a handshake is in progress causes OpenSSL to buffer an excessive amount of memory. This allows a peer to cause memory exhaustion, eventually resulting in a denial of service, using a small amount of network traffic.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-55654 — openssh@9.9p1

A flaw was found in OpenSSH. This vulnerability, a heap out-of-bounds read, occurs during the cleanup of GSSAPI (Generic Security Service Application Programming Interface) indicators when a trailing NULL termination is missing in the auth-indicators array. A remote attacker, under specific configurations involving GSSAPI authentication and a Kerberos environment, could exploit this to cause the SSH authentication path to crash or abort. This leads to a denial of service (DoS), impacting the availability of the SSH service.

Fixed in: 0:9.9p1-9.el9_8

[low] CVE-2026-57062 — gnupg2@2.3.3-5.el9_7

A flaw in GnuPG's gpgsm component improperly handles the Cryptographic Message Syntax (CMS) format for AES-GCM. By accepting an authentication tag length of 4 bytes instead of the required 12 bytes, this vulnerability allows for a low-impact data integrity issue where the cryptographic validity of messages could be compromised.

[low] CVE-2026-6276 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl. This vulnerability allows for information disclosure when a custom `Host:` header is used in an initial HTTP request, and a subsequent request reuses the same connection without specifying a new `Host:` header. This can lead to libcurl incorrectly sending cookies intended for the first host to the second host, resulting in a cookie leak. This issue is categorized as an Origin Validation Error (CWE-346). Exploitation typically requires specific debugging configurations.

[low] CVE-2026-6276 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl. This vulnerability allows for information disclosure when a custom `Host:` header is used in an initial HTTP request, and a subsequent request reuses the same connection without specifying a new `Host:` header. This can lead to libcurl incorrectly sending cookies intended for the first host to the second host, resulting in a cookie leak. This issue is categorized as an Origin Validation Error (CWE-346). Exploitation typically requires specific debugging configurations.

[low] CVE-2026-63073 — openssl@1:3.5.5

A flaw was found in OpenSSL. A malicious CMP (Certificate Management Protocol) endpoint can send an unexpected distinguished name (DN) directly as the format string argument to ERR_raise_data(), causing the application to dereference and write to unrelated stack contents. This can lead to a crash in the CMP client, resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-63073 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. A malicious CMP (Certificate Management Protocol) endpoint can send an unexpected distinguished name (DN) directly as the format string argument to ERR_raise_data(), causing the application to dereference and write to unrelated stack contents. This can lead to a crash in the CMP client, resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-63074 — openssl@1:3.5.5

A flaw was found in OpenSSL. The CMP (Certificate Management Protocol) implementation does not clear cached additional certificates when an invalid message is received, leading to excessive memory consumption. This allows a malicious client to repeatedly send requests containing unique extra certificates to cause memory exhaustion, eventually resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-63074 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. The CMP (Certificate Management Protocol) implementation does not clear cached additional certificates when an invalid message is received, leading to excessive memory consumption. This allows a malicious client to repeatedly send requests containing unique extra certificates to cause memory exhaustion, eventually resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-63075 — openssl@1:3.5.5

A flaw was found in OpenSSL. The QUIC protocol implementation retains metadata for ACK-only packets for the lifetime of a connection, leading to excessive memory consumption. This allows a peer to repeatedly send ack-eliciting packets while not acknowledging ACK-only responses to cause memory exhaustion, eventually resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-63075 — openssl-libs@1:3.5.5-6.el9_8

A flaw was found in OpenSSL. The QUIC protocol implementation retains metadata for ACK-only packets for the lifetime of a connection, leading to excessive memory consumption. This allows a peer to repeatedly send ack-eliciting packets while not acknowledging ACK-only responses to cause memory exhaustion, eventually resulting in a denial of service.

Fixed in: 1:3.5.8-1.el9_8

[low] CVE-2026-6842 — nano@5.6.1

A flaw was found in nano. In environments with permissive umask settings, a local attacker can exploit incorrect directory permissions (0777 instead of 0700) for the `~/.local` directory. This allows the attacker to inject a malicious `.desktop` launcher, which could lead to unintended actions or information disclosure if the launcher is subsequently processed.

[low] CVE-2026-73281 — openssh@9.9p1

A flaw was found in OpenSSH's `ssh-agent` component. A misinteraction between agent locking and the `session-bind@openssh.com` extension allows operations intended for local execution to be performed remotely. This could enable a remote attacker to add PKCS#11 tokens or utilize keys with destination restrictions, bypassing intended security controls.

Fixed in: 0:9.9p1-11.el9_8

[low] CVE-2026-7383 — openssl@1:3.5.5

A flaw was found in OpenSSL. A signed integer overflow vulnerability exists when sizing the destination buffer for Unicode output. This can lead to a heap buffer overflow, which may result in a crash or potentially allow an attacker to execute arbitrary code. Exploitation requires an application to directly call specific functions with a large amount of attacker-controlled input.

Fixed in: 1:3.5.5-4.el9_8

[low] CVE-2026-75803 — openssl@1:3.5.5

A flaw in OpenSSL causes EVP_Cipher() to skip AEAD tag verification for ChaCha20-Poly1305 and AES-OCB ciphers when decrypting empty ciphertexts. This allows remote attackers to submit forged messages that affected applications incorrectly accept as valid.

[low] CVE-2026-75803 — openssl-libs@1:3.5.5-6.el9_8

A flaw in OpenSSL causes EVP_Cipher() to skip AEAD tag verification for ChaCha20-Poly1305 and AES-OCB ciphers when decrypting empty ciphertexts. This allows remote attackers to submit forged messages that affected applications incorrectly accept as valid.

[low] CVE-2026-80230 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl, a client-side URL transfer library. When public key pinning is configured, but standard peer verification is explicitly disabled, libcurl incorrectly allows connections to proceed without enforcing the public key pinning. This bypass enables unauthenticated connections that should have been rejected, potentially compromising the integrity of the connection.

[low] CVE-2026-80230 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl, a client-side URL transfer library. When public key pinning is configured, but standard peer verification is explicitly disabled, libcurl incorrectly allows connections to proceed without enforcing the public key pinning. This bypass enables unauthenticated connections that should have been rejected, potentially compromising the integrity of the connection.

[low] CVE-2026-82209 — curl-minimal@7.76.1-40.el9

A flaw was found in libcurl when libpsl support is enabled. A remote attacker could exploit this vulnerability by setting a `Set-Cookie` header with a `Domain` attribute that explicitly matches a public suffix. This improper handling causes libcurl to save the cookie with a wildcard domain scope, leading to the cookie being inappropriately sent to arbitrary sibling subdomains under the same public suffix. This could result in sensitive information disclosure.

[low] CVE-2026-82209 — libcurl-minimal@7.76.1-40.el9

A flaw was found in libcurl when libpsl support is enabled. A remote attacker could exploit this vulnerability by setting a `Set-Cookie` header with a `Domain` attribute that explicitly matches a public suffix. This improper handling causes libcurl to save the cookie with a wildcard domain scope, leading to the cookie being inappropriately sent to arbitrary sibling subdomains under the same public suffix. This could result in sensitive information disclosure.

[low] CVE-2026-89156 — pcre2@10.40-6.el9

A flaw was found in PCRE2. An attacker can provide invalid UTF (Unicode Transformation Format) data, leading to an out-of-bounds read during a Just-In-Time (JIT) fallback. This vulnerability could potentially result in a denial of service.

[low] CVE-2026-89156 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2. An attacker can provide invalid UTF (Unicode Transformation Format) data, leading to an out-of-bounds read during a Just-In-Time (JIT) fallback. This vulnerability could potentially result in a denial of service.

[low] CVE-2026-89160 — pcre2@10.40-6.el9

A flaw was found in PCRE2, a library for processing regular expressions. A remote attacker could exploit this vulnerability by providing a specially crafted input that triggers an out-of-bounds read during pattern matching with invalid UTF (Unicode Transformation Format) characters. This could lead to a denial of service, making the affected system or application unavailable.

[low] CVE-2026-89160 — pcre2-syntax@10.40-6.el9

A flaw was found in PCRE2, a library for processing regular expressions. A remote attacker could exploit this vulnerability by providing a specially crafted input that triggers an out-of-bounds read during pattern matching with invalid UTF (Unicode Transformation Format) characters. This could lead to a denial of service, making the affected system or application unavailable.

[low] CVE-2026-9076 — openssl@1:3.5.5

A flaw was found in OpenSSL. When processing attacker-supplied Cryptographic Message Syntax (CMS) data using password-based decryption, an attacker can choose a stream-mode Key Encryption Key (KEK) cipher. This can trigger a heap out-of-bounds read, potentially causing an application crash

and leading to a Denial of Service (DoS). This vulnerability does not require password knowledge and can be exploited before authentication.

Fixed in: 1:3.5.5-4.el9_8

[low] GHSA-2x5j-vhc8-9cwm (CVE-2025-8556) — github.com/cloudflare/circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results

Fixed in: 1.6.1

[low] GHSA-2x5j-vhc8-9cwm (CVE-2025-8556) — github.com/cloudflare/circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results

Fixed in: 1.6.1

[low] GHSA-4vq8-7jfc-9cvp (CVE-2025-54410) — github.com/docker/docker@v25.0.6+incompatible

Moby firewalld reload removes bridge network isolation

Fixed in: 25.0.13

[low] GHSA-4vq8-7jfc-9cvp (CVE-2025-54410) — github.com/docker/docker@v27.4.1+incompatible

Moby firewalld reload removes bridge network isolation

Fixed in: 28.0.0

[low] GHSA-72x6-4j93-7w86 (CVE-2026-61712) — github.com/moby/buildkit@v0.12.5

BuildKit has a possible runtime DoS via unbounded group parsing

Fixed in: 0.31.1

[low] GHSA-72x6-4j93-7w86 (CVE-2026-61712) — github.com/moby/buildkit@v0.16.0

BuildKit has a possible runtime DoS via unbounded group parsing

Fixed in: 0.31.1

[low] GHSA-8wmf-6v46-5gfg (CVE-2026-81870) — go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry-Go: Exporter config logging may leak endpoint URLs in info logs

Fixed in: 1.45.0

[low] GHSA-8wmf-6v46-5gfg (CVE-2026-81870) — go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry-Go: Exporter config logging may leak endpoint URLs in info logs

Fixed in: 1.45.0

[low] GHSA-gm2x-2g9h-ccm8 (CVE-2026-33762) — github.com/go-git/go-git/v5@v5.11.0

go-git missing validation decoding Index v4 files leads to panic

Fixed in: 5.17.1

[low] GHSA-gm2x-2g9h-ccm8 (CVE-2026-33762) — github.com/go-git/go-git/v5@v5.13.2

go-git missing validation decoding Index v4 files leads to panic

Fixed in: 5.17.1

[low] GHSA-m7cr-m3pv-hgrp (CVE-2026-45570) — github.com/go-git/go-git/v5@v5.11.0

go-git: Improper single-quote escaping in go-git SSH transport

Fixed in: 5.19.1

[low] GHSA-m7cr-m3pv-hgrp (CVE-2026-45570) — github.com/go-git/go-git/v5@v5.13.2

go-git: Improper single-quote escaping in go-git SSH transport

Fixed in: 5.19.1

[low] GHSA-q9hv-hpm4-hj6x (CVE-2026-1229) — github.com/cloudflare/circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[low] GHSA-q9hv-hpm4-hj6x (CVE-2026-1229) — github.com/cloudflare/circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[low] GHSA-q9hv-hpm4-hj6x (CVE-2026-1229) — github.com/cloudflare/circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[low] GHSA-wqqc-jjcq-vfxm (CVE-2026-54787) — github.com/sigstore/sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period

Fixed in: 1.2.1

[low] GHSA-wqqc-jjcq-vfxm (CVE-2026-54787) — github.com/sigstore/sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period

Fixed in: 1.2.1

[low] GO-2026-4403 (CVE-2025-22873) — stdlib@go1.22.12

It was possible to improperly access the parent directory of an os.Root by opening a filename ending in "../". For example, Root.Open("../") would open the parent directory of the Root. This escape only permits opening the parent directory itself, not ancestors of the parent or files contained within the parent.

Fixed in: 1.23.9

[low] GO-2026-4403 (CVE-2025-22873) — stdlib@go1.22.12

It was possible to improperly access the parent directory of an os.Root by opening a filename ending in "../". For example, Root.Open("../") would open the parent directory of the Root. This escape only permits opening the parent directory itself, not ancestors of the parent or files contained within the parent.

Fixed in: 1.23.9

[low] GO-2026-4403 (CVE-2025-22873) — stdlib@go1.23.6

It was possible to improperly access the parent directory of an os.Root by opening a filename ending in "../". For example, Root.Open("../") would open the parent directory of the Root. This escape only permits opening the parent directory itself, not ancestors of the parent or files contained within the

parent.

Fixed in: 1.23.9

[low] GO-2026-4403 (CVE-2025-22873) — stdlib@go1.23.6

It was possible to improperly access the parent directory of an os.Root by opening a filename ending in "../". For example, Root.Open("../") would open the parent directory of the Root. This escape only permits opening the parent directory itself, not ancestors of the parent or files contained within the parent.

Fixed in: 1.23.9

[low] GO-2026-4403 (CVE-2025-22873) — stdlib@go1.23.6

It was possible to improperly access the parent directory of an os.Root by opening a filename ending in "../". For example, Root.Open("../") would open the parent directory of the Root. This escape only permits opening the parent directory itself, not ancestors of the parent or files contained within the parent.

Fixed in: 1.23.9

[low] GO-2026-4529 (CVE-2026-24122) — github.com/sigstore/cosign/v2@v2.4.3

Cosign considered signatures valid with expired intermediate certificates when transparency log verification is skipped in github.com/sigstore/cosign

[low] GO-2026-4529 (CVE-2026-24122) — github.com/sigstore/cosign/v2@v2.4.3

Cosign considered signatures valid with expired intermediate certificates when transparency log verification is skipped in github.com/sigstore/cosign

[low] GO-2026-4602 (CVE-2026-27139) — stdlib@go1.22.12

On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.

Fixed in: 1.25.8

[low] GO-2026-4602 (CVE-2026-27139) — stdlib@go1.22.12

On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.

Fixed in: 1.25.8

[low] GO-2026-4602 (CVE-2026-27139) — stdlib@go1.23.6

On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.

Fixed in: 1.25.8

[low] GO-2026-4602 (CVE-2026-27139) — stdlib@go1.23.6

On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.

Fixed in: 1.25.8

[low] GO-2026-4602 (CVE-2026-27139) — stdlib@go1.23.6

On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.

Fixed in: 1.25.8

[low] GO-2026-4602 (CVE-2026-27139) — stdlib@go1.25.5

On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could reference a file outside of the Root in which the File was opened. The impact of this escape is limited to reading metadata provided by lstat from arbitrary locations on the filesystem without permitting reading or writing files outside the root.

Fixed in: 1.25.8

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.29.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.29.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.30.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.30.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.30.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.33.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[low] GO-2026-5024 (CVE-2026-39824) — golang.org/x/sys@v0.42.0

NewNTUnicodeString does not check for string length overflow. When provided with a string that overflows the maximum size of a NTUnicodeString (a 16-bit number of bytes), it returns a truncated string rather than an error.

Fixed in: 0.44.0

[unknown] GO-2026-4316 — github.com/go-chi/chi@v4.1.2+incompatible

Open redirect vulnerability in the RedirectSlashes middleware in github.com/go-chi/chi

[unknown] GO-2026-4316 — github.com/go-chi/chi@v4.1.2+incompatible

Open redirect vulnerability in the RedirectSlashes middleware in github.com/go-chi/chi

[unknown] GO-2026-5775 — github.com/go-chi/chi/v5@v5.1.0

Chi Middleware vulnerable to IP spoofing via X-Forwarded-For header in github.com/go-chi/chi

Fixed in: 5.3.0

[unknown] GO-2026-5775 — github.com/go-chi/chi/v5@v5.1.0

Chi Middleware vulnerable to IP spoofing via X-Forwarded-For header in github.com/go-chi/chi

Fixed in: 5.3.0

[unknown] GO-2026-5777 — github.com/go-chi/chi/v5@v5.1.0

Chi's RealIP Middleware allows IP spoofing via unvalidated X-Forwarded-For header in github.com/go-chi/chi

Fixed in: 5.3.0

[unknown] GO-2026-5777 — github.com/go-chi/chi/v5@v5.1.0

Chi's RealIP Middleware allows IP spoofing via unvalidated X-Forwarded-For header in github.com/go-chi/chi

Fixed in: 5.3.0

[unknown] GO-2026-5841 — github.com/klauspost/compress@v1.17.11

Providing a specially crafted dictionary to s2.NewDict and using it to encode data can make the encoder read out of bounds.

Fixed in: 1.18.7

[unknown] GO-2026-5841 — github.com/klauspost/compress@v1.17.11

Providing a specially crafted dictionary to s2.NewDict and using it to encode data can make the encoder read out of bounds.

Fixed in: 1.18.7

[unknown] GO-2026-5841 — github.com/klauspost/compress@v1.17.11

Providing a specially crafted dictionary to s2.NewDict and using it to encode data can make the encoder read out of bounds.

Fixed in: 1.18.7

[unknown] GO-2026-5841 — github.com/klauspost/compress@v1.17.11

Providing a specially crafted dictionary to s2.NewDict and using it to encode data can make the encoder read out of bounds.

Fixed in: 1.18.7

[unknown] GO-2026-5841 — github.com/klauspost/compress@v1.17.7

Providing a specially crafted dictionary to s2.NewDict and using it to encode data can make the encoder read out of bounds.

Fixed in: 1.18.7

[unknown] GO-2026-5841 — github.com/klauspost/compress@v1.18.4

Providing a specially crafted dictionary to s2.NewDict and using it to encode data can make the encoder read out of bounds.

Fixed in: 1.18.7

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.32.0

The golang.org/x/crypto/openpgp package is unsafe by design, has numerous known security issues, is not maintained, and should not be used. If you are required to interoperate with OpenPGP systems and need a maintained package, consider github.com/ProtonMail/go-crypto/openpgp which is a maintained fork that aims to be a drop-in replacement for this package.

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.33.0

The golang.org/x/crypto/openpgp package is unsafe by design, has numerous known security issues, is not maintained, and should not be used. If you are required to interoperate with OpenPGP systems and need a maintained package, consider github.com/ProtonMail/go-crypto/openpgp which is a maintained fork that aims to be a drop-in replacement for this package.

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.33.0

The golang.org/x/crypto/openpgp package is unsafe by design, has numerous known security issues, is not maintained, and should not be used. If you are required to interoperate with OpenPGP systems and need a maintained package, consider github.com/ProtonMail/go-crypto/openpgp which is a maintained fork that aims to be a drop-in replacement for this package.

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.39.0

The golang.org/x/crypto/openpgp package is unsafe by design, has numerous known security issues, is not maintained, and should not be used. If you are required to interoperate with OpenPGP systems and need a maintained package, consider github.com/ProtonMail/go-crypto/openpgp which is a maintained fork that aims to be a drop-in replacement for this package.

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.49.0

The golang.org/x/crypto/openpgp package is unsafe by design, has numerous known security issues, is not maintained, and should not be used. If you are required to interoperate with OpenPGP systems and need a maintained package, consider github.com/ProtonMail/go-crypto/openpgp which is a maintained fork that aims to be a drop-in replacement for this package.

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.53.0

The golang.org/x/crypto/openpgp package is unsafe by design, has numerous known security issues, is not maintained, and should not be used. If you are required to interoperate with OpenPGP systems and need a maintained package, consider github.com/ProtonMail/go-crypto/openpgp which is a maintained fork that aims to be a drop-in replacement for this package.

[unknown] GO-2026-6225 — github.com/chrismellard/docker-credential-acr-env@v0.0.0-20230304212654-82a0ddb27589

In github.com/chrismellard/docker-credential-acr-env/pkg/credhelper, the regular expression used by isACRRegistry to validate Azure Container Registry hostnames is unanchored. As a result, arbitrary

hostnames containing the substring ".azurecr.io" (such as evil.azurecr.io.attacker.com) are treated as valid ACR registries, causing ACRCredHelper.Get to send the Azure Active Directory (AAD) access token to attacker-controlled hosts.

[unknown] GO-2026-6225 — github.com/chrismellard/docker-credential-acr-env@v0.0.0-20230304212654-82a0ddb27589

In github.com/chrismellard/docker-credential-acr-env/pkg/credhelper, the regular expression used by isACRRegistry to validate Azure Container Registry hostnames is unanchored. As a result, arbitrary hostnames containing the substring ".azurecr.io" (such as evil.azurecr.io.attacker.com) are treated as valid ACR registries, causing ACRCredHelper.Get to send the Azure Active Directory (AAD) access token to attacker-controlled hosts.

[unknown] GO-2026-6225 — github.com/chrismellard/docker-credential-acr-env@v0.0.0-20230304212654-82a0ddb27589

In github.com/chrismellard/docker-credential-acr-env/pkg/credhelper, the regular expression used by isACRRegistry to validate Azure Container Registry hostnames is unanchored. As a result, arbitrary hostnames containing the substring ".azurecr.io" (such as evil.azurecr.io.attacker.com) are treated as valid ACR registries, causing ACRCredHelper.Get to send the Azure Active Directory (AAD) access token to attacker-controlled hosts.

Findings from trivy

[critical] CVE-2025-21613 — github.com/go-git/go-git/v5@v5.11.0

go-git: argument injection via the URL field

Fixed in: 5.13.0

[critical] CVE-2025-68121 — stdlib@1.22.12

crypto/tls: crypto/tls: Incorrect certificate validation during TLS session resumption

Fixed in: 1.24.13, 1.25.7, 1.26.0-rc.3

[critical] CVE-2025-68121 — stdlib@1.23.6

crypto/tls: crypto/tls: Incorrect certificate validation during TLS session resumption

Fixed in: 1.24.13, 1.25.7, 1.26.0-rc.3

[critical] CVE-2025-68121 — stdlib@1.25.5

crypto/tls: crypto/tls: Incorrect certificate validation during TLS session resumption

Fixed in: 1.24.13, 1.25.7, 1.26.0-rc.3

[critical] CVE-2026-33186 — google.golang.org/grpc@v1.67.1

google.golang.org/grpc/grpc-go: google.golang.org/grpc/authz: gRPC-Go: Authorization bypass due to improper HTTP/2 path validation

Fixed in: 1.79.3

[critical] CVE-2026-33186 — google.golang.org/grpc@v1.69.4

google.golang.org/grpc/grpc-go: google.golang.org/grpc/authz: gRPC-Go: Authorization bypass due to improper HTTP/2 path validation

Fixed in: 1.79.3

[critical] CVE-2026-33186 — google.golang.org/grpc@v1.70.0

google.golang.org/grpc/grpc-go: google.golang.org/grpc/authz: gRPC-Go: Authorization bypass due to

improper HTTP/2 path validation

Fixed in: 1.79.3

[high] CVE-2024-25621 — github.com/containerd/containerd@v1.7.11

github.com/containerd/containerd: containerd local privilege escalation

Fixed in: 1.7.29

[high] CVE-2025-15558 — github.com/docker/cli@v27.4.1+incompatible

docker/cli: Docker CLI for Windows: Privilege escalation via malicious plugin binaries

Fixed in: 29.2.0

[high] CVE-2025-15558 — github.com/docker/cli@v28.0.0+incompatible

docker/cli: Docker CLI for Windows: Privilege escalation via malicious plugin binaries

Fixed in: 29.2.0

[high] CVE-2025-21614 — github.com/go-git/go-git/v5@v5.11.0

go-git: go-git clients vulnerable to DoS via maliciously crafted Git server replies

Fixed in: 5.13.0

[high] CVE-2025-22868 — golang.org/x/oauth2@v0.12.0

golang.org/x/oauth2/jws: Unexpected memory consumption during token parsing in golang.org/x/oauth2/jws

Fixed in: 0.27.0

[high] CVE-2025-22868 — golang.org/x/oauth2@v0.18.0

golang.org/x/oauth2/jws: Unexpected memory consumption during token parsing in golang.org/x/oauth2/jws

Fixed in: 0.27.0

[high] CVE-2025-22868 — golang.org/x/oauth2@v0.23.0

golang.org/x/oauth2/jws: Unexpected memory consumption during token parsing in golang.org/x/oauth2/jws

Fixed in: 0.27.0

[high] CVE-2025-22868 — golang.org/x/oauth2@v0.26.0

golang.org/x/oauth2/jws: Unexpected memory consumption during token parsing in golang.org/x/oauth2/jws

Fixed in: 0.27.0

[high] CVE-2025-22869 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: Denial of Service in the Key Exchange of golang.org/x/crypto/ssh

Fixed in: 0.35.0

[high] CVE-2025-22869 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: Denial of Service in the Key Exchange of golang.org/x/crypto/ssh

Fixed in: 0.35.0

[high] CVE-2025-30204 — github.com/golang-jwt/jwt/v4@v4.5.1

golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing

Fixed in: 4.5.2

[high] CVE-2025-30204 — github.com/golang-jwt/jwt/v5@v5.2.1

golang-jwt/jwt: jwt-go allows excessive memory allocation during header parsing

Fixed in: 5.2.2

[high] CVE-2025-31133 — github.com/opencontainers/runc@v1.1.12

runc: container escape via 'masked path' abuse due to mount race conditions

Fixed in: 1.2.8, 1.3.3, 1.4.0-rc.3

[high] CVE-2025-47913 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: SSH client panic due to unexpected SSH_AGENT_SUCCESS

Fixed in: 0.43.0

[high] CVE-2025-47913 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: SSH client panic due to unexpected SSH_AGENT_SUCCESS

Fixed in: 0.43.0

[high] CVE-2025-47913 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: SSH client panic due to unexpected SSH_AGENT_SUCCESS

Fixed in: 0.43.0

[high] CVE-2025-52565 — github.com/opencontainers/runc@v1.1.12

runc: container escape with malicious config due to /dev/console mount and related races

Fixed in: 1.2.8, 1.3.3, 1.4.0-rc.3

[high] CVE-2025-52881 — github.com/opencontainers/runc@v1.1.12

runc: opencontainers/selinux: container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.2.8, 1.3.3, 1.4.0-rc.3

[high] CVE-2025-52881 — github.com/opencontainers/selinux@v1.11.0

runc: opencontainers/selinux: container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.13.0

[high] CVE-2025-61726 — stdlib@1.22.12

golang: net/url: Memory exhaustion in query parameter parsing in net/url

Fixed in: 1.24.12, 1.25.6

[high] CVE-2025-61726 — stdlib@1.23.6

golang: net/url: Memory exhaustion in query parameter parsing in net/url

Fixed in: 1.24.12, 1.25.6

[high] CVE-2025-61726 — stdlib@1.25.5

golang: net/url: Memory exhaustion in query parameter parsing in net/url

Fixed in: 1.24.12, 1.25.6

[high] CVE-2025-61729 — stdlib@1.22.12

crypto/x509: golang: Denial of Service due to excessive resource consumption via crafted certificate

Fixed in: 1.24.11, 1.25.5

[high] CVE-2025-61729 — stdlib@1.23.6

crypto/x509: golang: Denial of Service due to excessive resource consumption via crafted certificate

Fixed in: 1.24.11, 1.25.5

[high] CVE-2025-66506 — github.com/sigstore/fulcio@v1.4.3

github.com/sigstore/fulcio: Fulcio: Denial of Service via crafted OpenID Connect (OIDC) token

Fixed in: 1.8.3

[high] CVE-2025-66506 — github.com/sigstore/fulcio@v1.6.6

github.com/sigstore/fulcio: Fulcio: Denial of Service via crafted OpenID Connect (OIDC) token

Fixed in: 1.8.3

[high] CVE-2025-66564 — github.com/sigstore/timestamp-authority@v1.2.4

github.com/sigstore/timestamp-authority: Sigstore Timestamp Authority: Denial of Service via excessive OID or Content-Type header parsing

Fixed in: 2.0.3

[high] CVE-2026-24051 — go.opentelemetry.io/otel/sdk@v1.34.0

opentelemetry-go: OpenTelemetry-Go Affected by Arbitrary Code Execution via PATH Hijacking

Fixed in: 1.40.0

[high] CVE-2026-25679 — stdlib@1.22.12

net/url: Incorrect parsing of IPv6 host literals in net/url

Fixed in: 1.25.8, 1.26.1

[high] CVE-2026-25679 — stdlib@1.23.6

net/url: Incorrect parsing of IPv6 host literals in net/url

Fixed in: 1.25.8, 1.26.1

[high] CVE-2026-25679 — stdlib@1.25.5

net/url: Incorrect parsing of IPv6 host literals in net/url

Fixed in: 1.25.8, 1.26.1

[high] CVE-2026-25681 — golang.org/x/net@v0.33.0

golang.org/x/net/html: golang.org/x/net/html: Arbitrary code execution via Cross-Site Scripting

Fixed in: 0.55.0

[high] CVE-2026-25681 — golang.org/x/net@v0.34.0

golang.org/x/net/html: golang.org/x/net/html: Arbitrary code execution via Cross-Site Scripting

Fixed in: 0.55.0

[high] CVE-2026-25681 — golang.org/x/net@v0.35.0

golang.org/x/net/html: golang.org/x/net/html: Arbitrary code execution via Cross-Site Scripting

Fixed in: 0.55.0

[high] CVE-2026-25681 — golang.org/x/net@v0.41.0

golang.org/x/net/html: golang.org/x/net/html: Arbitrary code execution via Cross-Site Scripting

Fixed in: 0.55.0

[high] CVE-2026-25681 — golang.org/x/net@v0.52.0

golang.org/x/net/html: golang.org/x/net/html: Arbitrary code execution via Cross-Site Scripting

Fixed in: 0.55.0

[high] CVE-2026-27136 — golang.org/x/net@v0.33.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via HTML parsing bypass

Fixed in: 0.55.0

[high] CVE-2026-27136 — golang.org/x/net@v0.34.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via HTML parsing bypass

Fixed in: 0.55.0

[high] CVE-2026-27136 — golang.org/x/net@v0.35.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via HTML parsing bypass

Fixed in: 0.55.0

[high] CVE-2026-27136 — golang.org/x/net@v0.41.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via HTML parsing bypass

Fixed in: 0.55.0

[high] CVE-2026-27136 — golang.org/x/net@v0.52.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via HTML parsing bypass

Fixed in: 0.55.0

[high] CVE-2026-27145 — stdlib@1.22.12

crypto/x509: golang: golang crypto/x509: Denial of Service via excessive processing of DNS SAN entries

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-27145 — stdlib@1.23.6

crypto/x509: golang: golang crypto/x509: Denial of Service via excessive processing of DNS SAN entries

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-27145 — stdlib@1.25.5

crypto/x509: golang: golang crypto/x509: Denial of Service via excessive processing of DNS SAN entries

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-27145 — stdlib@1.25.9

crypto/x509: golang: golang crypto/x509: Denial of Service via excessive processing of DNS SAN entries

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-27145 — stdlib@1.26.2

crypto/x509: golang: golang crypto/x509: Denial of Service via excessive processing of DNS SAN entries

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-27896 — github.com/modelcontextprotocol/go-sdk@v1.1.0

modelcontextprotocol/go-sdk: improper handling of case sensitivity

Fixed in: 1.3.1

[high] CVE-2026-32280 — stdlib@1.22.12

crypto/x509: crypto/tls: golang: Go: Denial of Service vulnerability in certificate chain building

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32280 — stdlib@1.23.6

crypto/x509: crypto/tls: golang: Go: Denial of Service vulnerability in certificate chain building

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32280 — stdlib@1.25.5

crypto/x509: crypto/tls: golang: Go: Denial of Service vulnerability in certificate chain building

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32281 — stdlib@1.22.12

crypto/x509: golang: Go crypto/x509: Denial of Service via inefficient certificate chain validation

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32281 — stdlib@1.23.6

crypto/x509: golang: Go crypto/x509: Denial of Service via inefficient certificate chain validation

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32281 — stdlib@1.25.5

crypto/x509: golang: Go crypto/x509: Denial of Service via inefficient certificate chain validation

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32283 — stdlib@1.22.12

crypto/tls: golang: Go crypto/tls: Denial of Service via multiple TLS 1.3 key update messages

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32283 — stdlib@1.23.6

crypto/tls: golang: Go crypto/tls: Denial of Service via multiple TLS 1.3 key update messages

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-32283 — stdlib@1.25.5

crypto/tls: golang: Go crypto/tls: Denial of Service via multiple TLS 1.3 key update messages

Fixed in: 1.25.9, 1.26.2

[high] CVE-2026-33252 — github.com/modelcontextprotocol/go-sdk@v1.1.0

encoding/json: golang: github.com/modelcontextprotocol/go-sdk: Go MCP SDK: Remote tool execution via cross-site request forgery

Fixed in: 1.4.1

[high] CVE-2026-33540 — github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

github.com/distribution/distribution: Distribution: Information disclosure via improper validation of authentication realm URL

Fixed in: 3.1.0

[high] CVE-2026-33747 — github.com/moby/buildkit@v0.12.5

BuildKit: github.com/moby/buildkit: BuildKit: Arbitrary file write and code execution via untrusted frontend

Fixed in: 0.28.1

[high] CVE-2026-33747 — github.com/moby/buildkit@v0.16.0

BuildKit: github.com/moby/buildkit: BuildKit: Arbitrary file write and code execution via untrusted frontend

Fixed in: 0.28.1

[high] CVE-2026-33748 — github.com/moby/buildkit@v0.12.5

github.com/moby/buildkit: BuildKit: Unauthorized file access via Git URL fragment subdir components

Fixed in: 0.28.1

[high] CVE-2026-33748 — github.com/moby/buildkit@v0.16.0

github.com/moby/buildkit: BuildKit: Unauthorized file access via Git URL fragment subdir components

Fixed in: 0.28.1

[high] CVE-2026-33811 — stdlib@1.22.12

net: golang: Go net package: Denial of Service via long CNAME response in LookupCNAME

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33811 — stdlib@1.23.6

net: golang: Go net package: Denial of Service via long CNAME response in LookupCNAME

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33811 — stdlib@1.25.5

net: golang: Go net package: Denial of Service via long CNAME response in LookupCNAME

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33811 — stdlib@1.25.9

net: golang: Go net package: Denial of Service via long CNAME response in LookupCNAME

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33811 — stdlib@1.26.2

net: golang: Go net package: Denial of Service via long CNAME response in LookupCNAME

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33814 — golang.org/x/net@v0.33.0

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 0.53.0

[high] CVE-2026-33814 — golang.org/x/net@v0.34.0

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 0.53.0

[high] CVE-2026-33814 — golang.org/x/net@v0.35.0

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 0.53.0

[high] CVE-2026-33814 — golang.org/x/net@v0.41.0

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 0.53.0

[high] CVE-2026-33814 — golang.org/x/net@v0.52.0

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 0.53.0

[high] CVE-2026-33814 — stdlib@1.22.12

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33814 — stdlib@1.23.6

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33814 — stdlib@1.25.5

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33814 — stdlib@1.25.9

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33814 — stdlib@1.26.2

net/http/internal/http2: golang: golang.org/x/net: Go HTTP/2: Denial of Service via malformed SETTINGS_MAX_FRAME_SIZE frame

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-33818 — stdlib@1.22.12

encoding/asn1: golang: Go encoding/asn1: Denial of Service via excessive recursion in Unmarshal

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-33818 — stdlib@1.23.6

encoding/asn1: golang: Go encoding/asn1: Denial of Service via excessive recursion in Unmarshal

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-33818 — stdlib@1.25.5

encoding/asn1: golang: Go encoding/asn1: Denial of Service via excessive recursion in Unmarshal

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-33818 — stdlib@1.25.9

encoding/asn1: golang: Go encoding/asn1: Denial of Service via excessive recursion in Unmarshal

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-33818 — stdlib@1.26.2

encoding/asn1: golang: Go encoding/asn1: Denial of Service via excessive recursion in Unmarshal

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-33818 — stdlib@1.26.5

encoding/asn1: golang: Go encoding/asn1: Denial of Service via excessive recursion in Unmarshal

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-34040 — github.com/docker/docker@v25.0.6+incompatible

Moby: Moby: Authorization bypass vulnerability

Fixed in: 29.3.1

[high] CVE-2026-34040 — github.com/docker/docker@v27.4.1+incompatible

Moby: Moby: Authorization bypass vulnerability

Fixed in: 29.3.1

[high] CVE-2026-34040 — github.com/docker/docker@v28.0.0+incompatible

Moby: Moby: Authorization bypass vulnerability

Fixed in: 29.3.1

[high] CVE-2026-34742 — github.com/modelcontextprotocol/go-sdk@v1.1.0

github.com/modelcontextprotocol/go-sdk: Model Context Protocol (MCP) Go SDK: DNS rebinding vulnerability allows unauthorized access

Fixed in: 1.4.0

[high] CVE-2026-34986 — github.com/go-jose/go-jose/v3@v3.0.3

github.com/go-jose/go-jose/v3: github.com/go-jose/go-jose/v4: Go JOSE: Denial of Service via crafted JSON Web Encryption (JWE) object

Fixed in: 3.0.5

[high] CVE-2026-34986 — github.com/go-jose/go-jose/v4@v4.0.5

github.com/go-jose/go-jose/v3: github.com/go-jose/go-jose/v4: Go JOSE: Denial of Service via crafted JSON Web Encryption (JWE) object

Fixed in: 4.1.4

[high] CVE-2026-35172 —

github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

github.com/distribution/distribution: Distribution: Information disclosure via stale references after content deletion

Fixed in: 3.1.0

[high] CVE-2026-35469 — github.com/moby/spdystream@v0.2.0

Kubelet: CRI-O: kube-apiserver: Kubelet, CRI-O, kube-apiserver: Denial of Service via SPDY streaming code

Fixed in: 0.5.1

[high] CVE-2026-35469 — github.com/moby/spdystream@v0.4.0

Kubelet: CRI-O: kube-apiserver: Kubelet, CRI-O, kube-apiserver: Denial of Service via SPDY streaming code

Fixed in: 0.5.1

[high] CVE-2026-35469 — github.com/moby/spdystream@v0.5.0

Kubelet: CRI-O: kube-apiserver: Kubelet, CRI-O, kube-apiserver: Denial of Service via SPDY streaming code

Fixed in: 0.5.1

[high] CVE-2026-39820 — stdlib@1.22.12

net/mail: golang: Go net/mail: Denial of Service via crafted email inputs

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39820 — stdlib@1.23.6

net/mail: golang: Go net/mail: Denial of Service via crafted email inputs

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39820 — stdlib@1.25.5

net/mail: golang: Go net/mail: Denial of Service via crafted email inputs

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39820 — stdlib@1.25.9

net/mail: golang: Go net/mail: Denial of Service via crafted email inputs

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39820 — stdlib@1.26.2

net/mail: golang: Go net/mail: Denial of Service via crafted email inputs

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39821 — golang.org/x/net@v0.33.0

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 0.55.0

[high] CVE-2026-39821 — golang.org/x/net@v0.34.0

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 0.55.0

[high] CVE-2026-39821 — golang.org/x/net@v0.35.0

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 0.55.0

[high] CVE-2026-39821 — golang.org/x/net@v0.41.0

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 0.55.0

[high] CVE-2026-39821 — golang.org/x/net@v0.52.0

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 0.55.0

[high] CVE-2026-39821 — stdlib@1.22.12

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-39821 — stdlib@1.23.6

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-39821 — stdlib@1.25.5

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-39821 — stdlib@1.25.9

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-39821 — stdlib@1.26.2

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-39821 — stdlib@1.26.5

golang.org/x/net/idna: golang: net/http: golang.org/x/net/idna: Privilege escalation via incorrect Punycode label processing

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-39822 — stdlib@1.22.12

golang: Go os.Root: Symlink following vulnerability allows directory traversal

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[high] CVE-2026-39822 — stdlib@1.23.6

golang: Go os.Root: Symlink following vulnerability allows directory traversal

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[high] CVE-2026-39822 — stdlib@1.25.5

golang: Go os.Root: Symlink following vulnerability allows directory traversal

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[high] CVE-2026-39822 — stdlib@1.25.9

golang: Go os.Root: Symlink following vulnerability allows directory traversal

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[high] CVE-2026-39822 — stdlib@1.26.2

golang: Go os.Root: Symlink following vulnerability allows directory traversal

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[high] CVE-2026-39828 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Unauthorized command execution via discarded SSH permissions

Fixed in: 0.52.0

[high] CVE-2026-39828 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Unauthorized command execution via discarded SSH permissions

Fixed in: 0.52.0

[high] CVE-2026-39828 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Unauthorized command execution via discarded SSH permissions

Fixed in: 0.52.0

[high] CVE-2026-39828 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Unauthorized command execution via discarded SSH permissions

Fixed in: 0.52.0

[high] CVE-2026-39829 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted public key with excessive parameters

Fixed in: 0.52.0

[high] CVE-2026-39829 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted public key with excessive parameters

Fixed in: 0.52.0

[high] CVE-2026-39829 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted public key with excessive parameters

Fixed in: 0.52.0

[high] CVE-2026-39829 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted public key with excessive parameters

Fixed in: 0.52.0

[high] CVE-2026-39830 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via resource leak from unsolicited SSH responses

Fixed in: 0.52.0

[high] CVE-2026-39830 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via resource leak from unsolicited SSH responses

Fixed in: 0.52.0

[high] CVE-2026-39830 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via resource leak from unsolicited SSH responses

Fixed in: 0.52.0

[high] CVE-2026-39830 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via resource leak from unsolicited SSH responses

Fixed in: 0.52.0

[high] CVE-2026-39831 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Security key bypass due to missing user presence check

Fixed in: 0.52.0

[high] CVE-2026-39831 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Security key bypass due to missing user presence check

Fixed in: 0.52.0

[high] CVE-2026-39831 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Security key bypass due to missing user presence check

Fixed in: 0.52.0

[high] CVE-2026-39831 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Security key bypass due to missing user presence check

Fixed in: 0.52.0

[high] CVE-2026-39832 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to improper handling of key restrictions

Fixed in: 0.52.0

[high] CVE-2026-39832 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to improper handling of key restrictions

Fixed in: 0.52.0

[high] CVE-2026-39832 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to improper handling of key restrictions

Fixed in: 0.52.0

[high] CVE-2026-39832 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to improper handling of key restrictions

Fixed in: 0.52.0

[high] CVE-2026-39835 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via crafted SSH certificate

Fixed in: 0.52.0

[high] CVE-2026-39835 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via crafted SSH certificate

Fixed in: 0.52.0

[high] CVE-2026-39835 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via crafted SSH certificate

Fixed in: 0.52.0

[high] CVE-2026-39835 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via crafted SSH certificate

Fixed in: 0.52.0

[high] CVE-2026-39836 — stdlib@1.22.12

net: golang: Go net package: Denial of Service via NUL byte in Dial and LookupPort on Windows

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39836 — stdlib@1.23.6

net: golang: Go net package: Denial of Service via NUL byte in Dial and LookupPort on Windows

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39836 — stdlib@1.25.5

net: golang: Go net package: Denial of Service via NUL byte in Dial and LookupPort on Windows

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39836 — stdlib@1.25.9

net: golang: Go net package: Denial of Service via NUL byte in Dial and LookupPort on Windows

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39836 — stdlib@1.26.2

net: golang: Go net package: Denial of Service via NUL byte in Dial and LookupPort on Windows

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-39883 — go.opentelemetry.io/otel/sdk@v1.34.0

github.com/open-telemetry/opentelemetry-go: OpenTelemetry-Go: Arbitrary code execution via PATH hijacking on BSD/Solaris

Fixed in: 1.43.0

[high] CVE-2026-41567 — github.com/docker/docker@v25.0.6+incompatible

docker: Moby/Docker Engine: Arbitrary Code Execution via malicious container image and compressed archive upload

[high] CVE-2026-41567 — github.com/docker/docker@v27.4.1+incompatible

docker: Moby/Docker Engine: Arbitrary Code Execution via malicious container image and compressed archive upload

[high] CVE-2026-41567 — github.com/docker/docker@v28.0.0+incompatible

docker: Moby/Docker Engine: Arbitrary Code Execution via malicious container image and compressed archive upload

[high] CVE-2026-42306 — github.com/docker/docker@v25.0.6+incompatible

github.com/docker/docker: github.com/moby/moby: Moby container framework: Host file overwrite via race condition in docker cp mount setup

[high] CVE-2026-42306 — github.com/docker/docker@v27.4.1+incompatible

github.com/docker/docker: github.com/moby/moby: Moby container framework: Host file overwrite via race condition in docker cp mount setup

[high] CVE-2026-42306 — github.com/docker/docker@v28.0.0+incompatible

github.com/docker/docker: github.com/moby/moby: Moby container framework: Host file overwrite via race condition in docker cp mount setup

[high] CVE-2026-42499 — stdlib@1.22.12

net/mail: golang: net/mail: Denial of Service via pathological email address parsing

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-42499 — stdlib@1.23.6

net/mail: golang: net/mail: Denial of Service via pathological email address parsing

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-42499 — stdlib@1.25.5

net/mail: golang: net/mail: Denial of Service via pathological email address parsing

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-42499 — stdlib@1.25.9

net/mail: golang: net/mail: Denial of Service via pathological email address parsing

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-42499 — stdlib@1.26.2

net/mail: golang: net/mail: Denial of Service via pathological email address parsing

Fixed in: 1.25.10, 1.26.3

[high] CVE-2026-42504 — stdlib@1.22.12

mime: golang: Golang MIME: Denial of Service via maliciously-crafted MIME header

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-42504 — stdlib@1.23.6

mime: golang: Golang MIME: Denial of Service via maliciously-crafted MIME header

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-42504 — stdlib@1.25.5

mime: golang: Golang MIME: Denial of Service via maliciously-crafted MIME header

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-42504 — stdlib@1.25.9

mime: golang: Golang MIME: Denial of Service via maliciously-crafted MIME header

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-42504 — stdlib@1.26.2

mime: golang: Golang MIME: Denial of Service via maliciously-crafted MIME header

Fixed in: 1.25.11, 1.26.4

[high] CVE-2026-42508 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/knownhosts: golang: golang.org/x/crypto/ssh/knownhosts: Revocation bypass via unchecked SignatureKey

Fixed in: 0.52.0

[high] CVE-2026-42508 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/knownhosts: golang: golang.org/x/crypto/ssh/knownhosts: Revocation bypass via unchecked SignatureKey

Fixed in: 0.52.0

[high] CVE-2026-42508 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/knownhosts: golang: golang.org/x/crypto/ssh/knownhosts: Revocation bypass via unchecked SignatureKey

Fixed in: 0.52.0

[high] CVE-2026-42508 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh/knownhosts: golang: golang.org/x/crypto/ssh/knownhosts: Revocation bypass via unchecked SignatureKey

Fixed in: 0.52.0

[high] CVE-2026-44973 — github.com/go-git/go-billy/v5@v5.5.0

github.com/go-git/go-billy: Go-billy: Arbitrary file access due to path traversal vulnerability

Fixed in: 5.9.0

[high] CVE-2026-44973 — github.com/go-git/go-billy/v5@v5.6.2

github.com/go-git/go-billy: Go-billy: Arbitrary file access due to path traversal vulnerability

Fixed in: 5.9.0

[high] CVE-2026-45022 — github.com/go-git/go-git/v5@v5.11.0

go-git is an extensible git implementation library written in pure Go. ...

Fixed in: 5.19.0

[high] CVE-2026-45022 — github.com/go-git/go-git/v5@v5.13.2

go-git is an extensible git implementation library written in pure Go. ...

Fixed in: 5.19.0

[high] CVE-2026-46595 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Authorization bypass due to skipped source-address validation

Fixed in: 0.52.0

[high] CVE-2026-46595 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Authorization bypass due to skipped source-address validation

Fixed in: 0.52.0

[high] CVE-2026-46595 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Authorization bypass due to skipped source-address validation

Fixed in: 0.52.0

[high] CVE-2026-46595 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Authorization bypass due to skipped source-address validation

Fixed in: 0.52.0

[high] CVE-2026-46597 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted AES-GCM packet decoder inputs

Fixed in: 0.52.0

[high] CVE-2026-46597 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted AES-GCM packet decoder inputs

Fixed in: 0.52.0

[high] CVE-2026-46597 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted AES-GCM packet decoder inputs

Fixed in: 0.52.0

[high] CVE-2026-46597 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via crafted AES-GCM packet decoder inputs

Fixed in: 0.52.0

[high] CVE-2026-46600 — golang.org/x/net@v0.33.0

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 0.56.0

[high] CVE-2026-46600 — golang.org/x/net@v0.34.0

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 0.56.0

[high] CVE-2026-46600 — golang.org/x/net@v0.35.0

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 0.56.0

[high] CVE-2026-46600 — golang.org/x/net@v0.41.0

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 0.56.0

[high] CVE-2026-46600 — golang.org/x/net@v0.52.0

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 0.56.0

[high] CVE-2026-46600 — golang.org/x/net@v0.55.0

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 0.56.0

[high] CVE-2026-46600 — stdlib@1.26.2

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 1.26.6, 1.27.0-rc.3

[high] CVE-2026-46600 — stdlib@1.26.5

golang.org/x/net/dns/dnsmessage: golang.org/x/net/dns/dnsmessage: Denial of Service via invalid DNS record parsing

Fixed in: 1.26.6, 1.27.0-rc.3

[high] CVE-2026-48702 — github.com/sigstore/rekor@v1.2.2

github.com/sigstore/rekor: Rekor: Denial of Service due to unbounded gzip decompression in Alpine APK parsing

Fixed in: 1.5.2

[high] CVE-2026-48702 — github.com/sigstore/rekor@v1.3.9

github.com/sigstore/rekor: Rekor: Denial of Service due to unbounded gzip decompression in Alpine APK parsing

Fixed in: 1.5.2

[high] CVE-2026-49478 — github.com/sigstore/fulcio@v1.4.3

github.com/sigstore/fulcio: Fulcio: Server-Side Request Forgery and Kubernetes ServiceAccount token leakage

Fixed in: 1.8.6

[high] CVE-2026-49478 — github.com/sigstore/fulcio@v1.6.6

github.com/sigstore/fulcio: Fulcio: Server-Side Request Forgery and Kubernetes ServiceAccount token leakage

Fixed in: 1.8.6

[high] CVE-2026-50163 — oras.land/oras-go/v2@v2.6.1

oras-go: Oras-go: Information disclosure and arbitrary file access via crafted tarball hardlinks

Fixed in: 2.6.2

[high] CVE-2026-53488 — github.com/containerd/containerd@v1.7.11

github.com/containerd/containerd: containerd: Host-root command execution via unvalidated image config labels in CRI plugin

Fixed in: 1.7.33

[high] CVE-2026-53488 — github.com/containerd/containerd@v1.7.32

github.com/containerd/containerd: containerd: Host-root command execution via unvalidated image config labels in CRI plugin

Fixed in: 1.7.33

[high] CVE-2026-54167 — github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

Fixed in: 0.48.0, 0.42.1, 0.39.6, 0.37.8

[high] CVE-2026-54167 — github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

Fixed in: 0.48.0, 0.42.1, 0.39.6, 0.37.8

[high] CVE-2026-56852 — golang.org/x/text@v0.21.0

golang.org/x/text: golang.org/x/text: Denial of Service via invalid UTF-8 input

Fixed in: 0.39.0

[high] CVE-2026-56852 — golang.org/x/text@v0.22.0

golang.org/x/text: golang.org/x/text: Denial of Service via invalid UTF-8 input

Fixed in: 0.39.0

[high] CVE-2026-56852 — golang.org/x/text@v0.26.0

golang.org/x/text: golang.org/x/text: Denial of Service via invalid UTF-8 input

Fixed in: 0.39.0

[high] CVE-2026-56852 — golang.org/x/text@v0.35.0

golang.org/x/text: golang.org/x/text: Denial of Service via invalid UTF-8 input

Fixed in: 0.39.0

[high] CVE-2026-56852 — golang.org/x/text@v0.37.0

golang.org/x/text: golang.org/x/text: Denial of Service via invalid UTF-8 input

Fixed in: 0.39.0

[high] CVE-2026-56852 — golang.org/x/text@v0.38.0

golang.org/x/text: golang.org/x/text: Denial of Service via invalid UTF-8 input

Fixed in: 0.39.0

[high] CVE-2026-56853 — stdlib@1.22.12

net/http: golang: Go net/http: Unencrypted HTTP/2 connections vulnerable to Denial of Service

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56853 — stdlib@1.23.6

net/http: golang: Go net/http: Unencrypted HTTP/2 connections vulnerable to Denial of Service

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56853 — stdlib@1.25.5

net/http: golang: Go net/http: Unencrypted HTTP/2 connections vulnerable to Denial of Service

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56853 — stdlib@1.25.9

net/http: golang: Go net/http: Unencrypted HTTP/2 connections vulnerable to Denial of Service

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56853 — stdlib@1.26.2

net/http: golang: Go net/http: Unencrypted HTTP/2 connections vulnerable to Denial of Service

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56853 — stdlib@1.26.5

net/http: golang: Go net/http: Unencrypted HTTP/2 connections vulnerable to Denial of Service

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56858 — stdlib@1.22.12

html/template: golang: Go html/template: Cross-Site Scripting via pathological input

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56858 — stdlib@1.23.6

html/template: golang: Go html/template: Cross-Site Scripting via pathological input

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56858 — stdlib@1.25.5

html/template: golang: Go html/template: Cross-Site Scripting via pathological input

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56858 — stdlib@1.25.9

html/template: golang: Go html/template: Cross-Site Scripting via pathological input

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56858 — stdlib@1.26.2

html/template: golang: Go html/template: Cross-Site Scripting via pathological input

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56858 — stdlib@1.26.5

html/template: golang: Go html/template: Cross-Site Scripting via pathological input

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56859 — stdlib@1.22.12

encoding/xml: golang: Go: Denial of Service via XML decoding recursion depth issue

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56859 — stdlib@1.23.6

encoding/xml: golang: Go: Denial of Service via XML decoding recursion depth issue

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56859 — stdlib@1.25.5

encoding/xml: golang: Go: Denial of Service via XML decoding recursion depth issue

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56859 — stdlib@1.25.9

encoding/xml: golang: Go: Denial of Service via XML decoding recursion depth issue

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56859 — stdlib@1.26.2

encoding/xml: golang: Go: Denial of Service via XML decoding recursion depth issue

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56859 — stdlib@1.26.5

encoding/xml: golang: Go: Denial of Service via XML decoding recursion depth issue

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56860 — stdlib@1.22.12

net/url: golang: golang net/url: Denial of Service from quadratic complexity in path resolution

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56860 — stdlib@1.23.6

net/url: golang: golang net/url: Denial of Service from quadratic complexity in path resolution

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56860 — stdlib@1.25.5

net/url: golang: golang net/url: Denial of Service from quadratic complexity in path resolution

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56860 — stdlib@1.25.9

net/url: golang: golang net/url: Denial of Service from quadratic complexity in path resolution

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56860 — stdlib@1.26.2

net/url: golang: golang net/url: Denial of Service from quadratic complexity in path resolution

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56860 — stdlib@1.26.5

net/url: golang: golang net/url: Denial of Service from quadratic complexity in path resolution

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56862 — stdlib@1.22.12

crypto/tls: golang: Golang crypto/tls: Denial of Service via indefinite KeyUpdate messages

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56862 — stdlib@1.23.6

crypto/tls: golang: Golang crypto/tls: Denial of Service via indefinite KeyUpdate messages

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56862 — stdlib@1.25.5

crypto/tls: golang: Golang crypto/tls: Denial of Service via indefinite KeyUpdate messages

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56862 — stdlib@1.25.9

crypto/tls: golang: Golang crypto/tls: Denial of Service via indefinite KeyUpdate messages

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56862 — stdlib@1.26.2

crypto/tls: golang: Golang crypto/tls: Denial of Service via indefinite KeyUpdate messages

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56862 — stdlib@1.26.5

crypto/tls: golang: Golang crypto/tls: Denial of Service via indefinite KeyUpdate messages

Fixed in: 1.25.13, 1.26.6, 1.27.0-rc.3

[high] CVE-2026-56864 — golang.org/x/mod@v0.22.0

A malicious GOSUMDB was capable of serving arbitrary module content no ...

Fixed in: 0.40.0

[high] CVE-2026-56864 — golang.org/x/mod@v0.25.0

A malicious GOSUMDB was capable of serving arbitrary module content no ...

Fixed in: 0.40.0

[high] CVE-2026-56864 — golang.org/x/mod@v0.33.0

A malicious GOSUMDB was capable of serving arbitrary module content no ...

Fixed in: 0.40.0

[high] CVE-2026-56865 — golang.org/x/mod@v0.22.0

A malicious GOPROXY was previously capable of forging up to two sumdb ...

Fixed in: 0.40.0

[high] CVE-2026-56865 — golang.org/x/mod@v0.25.0

A malicious GOPROXY was previously capable of forging up to two sumdb ...

Fixed in: 0.40.0

[high] CVE-2026-56865 — golang.org/x/mod@v0.33.0

A malicious GOPROXY was previously capable of forging up to two sumdb ...

Fixed in: 0.40.0

[high] CVE-2026-71556 — github.com/go-git/go-git/v5@v5.11.0

github.com/go-git/go-git/v5: go-git: Arbitrary file read/write via symbolic link resolution

Fixed in: 5.19.2

[high] CVE-2026-71556 — github.com/go-git/go-git/v5@v5.13.2

github.com/go-git/go-git/v5: go-git: Arbitrary file read/write via symbolic link resolution

Fixed in: 5.19.2

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.67.1

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.69.4

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.79.3

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-hrxh-6v49-42gf — google.golang.org/grpc@v1.80.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[high] GHSA-q382-vc8q-7jhj — github.com/modelcontextprotocol/go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

Fixed in: 1.4.1

[medium] CVE-2024-40635 — github.com/containerd/containerd@v1.7.11

containerd: containerd has an integer overflow in User ID handling

Fixed in: 1.7.27, 1.6.38

[medium] CVE-2024-45310 — github.com/opencontainers/runc@v1.1.12

runc: runc can be tricked into creating empty files/directories on host

Fixed in: 1.1.14, 1.2.0-rc.3

[medium] CVE-2024-45339 — github.com/golang/glog@v1.2.2

github.com/golang/glog: Vulnerability when creating log files in github.com/golang/glog

Fixed in: 1.2.4

[medium] CVE-2025-0913 — stdlib@1.22.12

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

Fixed in: 1.23.10, 1.24.4

[medium] CVE-2025-0913 — stdlib@1.23.6

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

Fixed in: 1.23.10, 1.24.4

[medium] CVE-2025-22870 — golang.org/x/net@v0.33.0

golang.org/x/net/proxy: golang.org/x/net/http/httpproxy: HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] CVE-2025-22870 — golang.org/x/net@v0.34.0

golang.org/x/net/proxy: golang.org/x/net/http/httpproxy: HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] CVE-2025-22870 — golang.org/x/net@v0.35.0

golang.org/x/net/proxy: golang.org/x/net/http/httpproxy: HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[medium] CVE-2025-22870 — stdlib@1.22.12

golang.org/x/net/proxy: golang.org/x/net/http/httpproxy: HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 1.23.7, 1.24.1

[medium] CVE-2025-22870 — stdlib@1.23.6

golang.org/x/net/proxy: golang.org/x/net/http/httpproxy: HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 1.23.7, 1.24.1

[medium] CVE-2025-22871 — stdlib@1.22.12

net/http: Request smuggling due to acceptance of invalid chunked data in net/http

Fixed in: 1.23.8, 1.24.2

[medium] CVE-2025-22871 — stdlib@1.23.6

net/http: Request smuggling due to acceptance of invalid chunked data in net/http

Fixed in: 1.23.8, 1.24.2

[medium] CVE-2025-22872 — golang.org/x/net@v0.33.0

golang.org/x/net/html: Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

Fixed in: 0.38.0

[medium] CVE-2025-22872 — golang.org/x/net@v0.34.0

golang.org/x/net/html: Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

Fixed in: 0.38.0

[medium] CVE-2025-22872 — golang.org/x/net@v0.35.0

golang.org/x/net/html: Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

Fixed in: 0.38.0

[medium] CVE-2025-22873 — stdlib@1.22.12

os: os: Information disclosure via path traversal using specially crafted filenames

Fixed in: 1.23.9, 1.24.3

[medium] CVE-2025-22873 — stdlib@1.23.6

os: os: Information disclosure via path traversal using specially crafted filenames

Fixed in: 1.23.9, 1.24.3

[medium] CVE-2025-27144 — github.com/go-jose/go-jose/v3@v3.0.3

go-jose: Go JOSE's Parsing Vulnerable to Denial of Service

Fixed in: 3.0.4

[medium] CVE-2025-4673 — stdlib@1.22.12

net/http: Sensitive headers not cleared on cross-origin redirect in net/http

Fixed in: 1.23.10, 1.24.4

[medium] CVE-2025-4673 — stdlib@1.23.6

net/http: Sensitive headers not cleared on cross-origin redirect in net/http

Fixed in: 1.23.10, 1.24.4

[medium] CVE-2025-47906 — stdlib@1.22.12

os/exec: Unexpected paths returned from LookPath in os/exec

Fixed in: 1.23.12, 1.24.6

[medium] CVE-2025-47906 — stdlib@1.23.6

os/exec: Unexpected paths returned from LookPath in os/exec

Fixed in: 1.23.12, 1.24.6

[medium] CVE-2025-47907 — stdlib@1.22.12

database/sql: Postgres Scan Race Condition

Fixed in: 1.23.12, 1.24.6

[medium] CVE-2025-47907 — stdlib@1.23.6

database/sql: Postgres Scan Race Condition

Fixed in: 1.23.12, 1.24.6

[medium] CVE-2025-47911 — golang.org/x/net@v0.33.0

golang.org/x/net/html: Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[medium] CVE-2025-47911 — golang.org/x/net@v0.34.0

golang.org/x/net/html: Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[medium] CVE-2025-47911 — golang.org/x/net@v0.35.0

golang.org/x/net/html: Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[medium] CVE-2025-47911 — golang.org/x/net@v0.41.0

golang.org/x/net/html: Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[medium] CVE-2025-47912 — stdlib@1.22.12

net/url: Insufficient validation of bracketed IPv6 hostnames in net/url

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-47912 — stdlib@1.23.6

net/url: Insufficient validation of bracketed IPv6 hostnames in net/url

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-47914 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent: SSH Agent servers: Denial of Service due to malformed messages

Fixed in: 0.45.0

[medium] CVE-2025-47914 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent: SSH Agent servers: Denial of Service due to malformed messages

Fixed in: 0.45.0

[medium] CVE-2025-47914 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent: SSH Agent servers: Denial of Service due to malformed messages

Fixed in: 0.45.0

[medium] CVE-2025-58058 — github.com/ulikunitz/xz@v0.5.11

github.com/ulikunitz/xz: github.com/ulikunitz/xz leaks memory

Fixed in: 0.5.15

[medium] CVE-2025-58181 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via unbounded memory consumption in GSSAPI authentication

Fixed in: 0.45.0

[medium] CVE-2025-58181 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via unbounded memory consumption in GSSAPI authentication

Fixed in: 0.45.0

[medium] CVE-2025-58181 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang.org/x/crypto/ssh: Denial of Service via unbounded memory consumption in GSSAPI authentication

Fixed in: 0.45.0

[medium] CVE-2025-58183 — stdlib@1.22.12

golang: archive/tar: Unbounded allocation when parsing GNU sparse map

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58183 — stdlib@1.23.6

golang: archive/tar: Unbounded allocation when parsing GNU sparse map

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58185 — stdlib@1.22.12

encoding/asn1: Parsing DER payload can cause memory exhaustion in encoding/asn1

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58185 — stdlib@1.23.6

encoding/asn1: Parsing DER payload can cause memory exhaustion in encoding/asn1

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58187 — stdlib@1.22.12

crypto/x509: Quadratic complexity when checking name constraints in crypto/x509

Fixed in: 1.24.9, 1.25.3

[medium] CVE-2025-58187 — stdlib@1.23.6

crypto/x509: Quadratic complexity when checking name constraints in crypto/x509

Fixed in: 1.24.9, 1.25.3

[medium] CVE-2025-58188 — stdlib@1.22.12

crypto/x509: golang: Panic when validating certificates with DSA public keys in crypto/x509

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58188 — stdlib@1.23.6

crypto/x509: golang: Panic when validating certificates with DSA public keys in crypto/x509

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58189 — stdlib@1.22.12

crypto/tls: go crypto/tls ALPN negotiation error contains attacker controlled information

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58189 — stdlib@1.23.6

crypto/tls: go crypto/tls ALPN negotiation error contains attacker controlled information

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-58190 — golang.org/x/net@v0.33.0

golang.org/x/net/html: Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[medium] CVE-2025-58190 — golang.org/x/net@v0.34.0

golang.org/x/net/html: Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[medium] CVE-2025-58190 — golang.org/x/net@v0.35.0

golang.org/x/net/html: Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[medium] CVE-2025-58190 — golang.org/x/net@v0.41.0

golang.org/x/net/html: Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[medium] CVE-2025-61723 — stdlib@1.22.12

encoding/pem: Quadratic complexity when parsing some invalid inputs in encoding/pem

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-61723 — stdlib@1.23.6

encoding/pem: Quadratic complexity when parsing some invalid inputs in encoding/pem

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-61724 — stdlib@1.22.12

net/textproto: Excessive CPU consumption in Reader.ReadResponse in net/textproto

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-61724 — stdlib@1.23.6

net/textproto: Excessive CPU consumption in Reader.ReadResponse in net/textproto

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-61725 — stdlib@1.22.12

net/mail: Excessive CPU consumption in ParseAddress in net/mail

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-61725 — stdlib@1.23.6

net/mail: Excessive CPU consumption in ParseAddress in net/mail

Fixed in: 1.24.8, 1.25.2

[medium] CVE-2025-61727 — stdlib@1.22.12

golang: crypto/x509: excluded subdomain constraint does not restrict wildcard SANs

Fixed in: 1.24.11, 1.25.5

[medium] CVE-2025-61727 — stdlib@1.23.6

golang: crypto/x509: excluded subdomain constraint does not restrict wildcard SANs

Fixed in: 1.24.11, 1.25.5

[medium] CVE-2025-61728 — stdlib@1.22.12

golang: archive/zip: Excessive CPU consumption when building archive index in archive/zip

Fixed in: 1.24.12, 1.25.6

[medium] CVE-2025-61728 — stdlib@1.23.6

golang: archive/zip: Excessive CPU consumption when building archive index in archive/zip

Fixed in: 1.24.12, 1.25.6

[medium] CVE-2025-61728 — stdlib@1.25.5

golang: archive/zip: Excessive CPU consumption when building archive index in archive/zip

Fixed in: 1.24.12, 1.25.6

[medium] CVE-2025-61730 — stdlib@1.22.12

crypto/tls: Handshake messages may be processed at the incorrect encryption level in crypto/tls

Fixed in: 1.24.12, 1.25.6

[medium] CVE-2025-61730 — stdlib@1.23.6

crypto/tls: Handshake messages may be processed at the incorrect encryption level in crypto/tls

Fixed in: 1.24.12, 1.25.6

[medium] CVE-2025-61730 — stdlib@1.25.5

crypto/tls: Handshake messages may be processed at the incorrect encryption level in crypto/tls

Fixed in: 1.24.12, 1.25.6

[medium] CVE-2025-64329 — github.com/containerd/containerd@v1.7.11

github.com/containerd/containerd: containerd: Memory exhaustion via CRI Attach implementation goroutine leaks

Fixed in: 1.7.29

[medium] CVE-2026-22703 — github.com/sigstore/cosign/v2@v2.4.3

github.com/sigstore/cosign: Cosign verification accepts any valid Rekor entry under certain conditions

Fixed in: 2.6.2

[medium] CVE-2026-22772 — github.com/sigstore/fulcio@v1.4.3

fulcio: Fulcio: Server-Side Request Forgery (SSRF) via unanchored regex in MetaIssuer URL validation

Fixed in: 1.8.5

[medium] CVE-2026-22772 — github.com/sigstore/fulcio@v1.6.6

fulcio: Fulcio: Server-Side Request Forgery (SSRF) via unanchored regex in MetaIssuer URL validation

Fixed in: 1.8.5

[medium] CVE-2026-2303 — go.mongodb.org/mongo-driver@v1.14.0

CVE-2026-2303 affecting package telegraf for versions less than 1.29.4-21

Fixed in: 1.17.7

[medium] CVE-2026-2303 — go.mongodb.org/mongo-driver@v1.16.1

CVE-2026-2303 affecting package telegraf for versions less than 1.29.4-21

Fixed in: 1.17.7

[medium] CVE-2026-23831 — github.com/sigstore/rekor@v1.2.2

github.com/sigstore/rekor: Rekor denial of service

Fixed in: 1.5.0

[medium] CVE-2026-23831 — github.com/sigstore/rekor@v1.3.9

github.com/sigstore/rekor: Rekor denial of service

Fixed in: 1.5.0

[medium] CVE-2026-23991 — github.com/theupdateframework/go-tuf/v2@v2.0.2

github.com/theupdateframework/go-tuf/v2: go-tuf client DoS via malformed server response

Fixed in: 2.3.1

[medium] CVE-2026-23992 — github.com/theupdateframework/go-tuf/v2@v2.0.2

github.com/theupdateframework/go-tuf/v2: go-tuf improperly validates the configured threshold for

delegations

Fixed in: 2.3.1

[medium] CVE-2026-24117 — github.com/sigstore/rekor@v1.2.2

github.com/sigstore/rekor: Rekor Server-Side Request Forgery (SSRF)

Fixed in: 1.5.0

[medium] CVE-2026-24117 — github.com/sigstore/rekor@v1.3.9

github.com/sigstore/rekor: Rekor Server-Side Request Forgery (SSRF)

Fixed in: 1.5.0

[medium] CVE-2026-24137 — github.com/sigstore/sigstore@v1.8.15

github.com/sigstore/sigstore: sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[medium] CVE-2026-24137 — github.com/sigstore/sigstore@v1.8.2

github.com/sigstore/sigstore: sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[medium] CVE-2026-24686 — github.com/theupdateframework/go-tuf/v2@v2.0.2

github.com/theupdateframework/go-tuf/v2: go-tuf Path Traversal in TAP 4 Multirepo Client Allows Arbitrary File Write via Malicious Repository Names

Fixed in: 2.4.1

[medium] CVE-2026-25542 — github.com/tektoncd/pipeline@v0.65.1

github.com/tektoncd/pipeline: Tekton Pipelines: Security bypass due to regular expression matching flaw

Fixed in: 1.0.2, 1.3.4, 1.6.2, 1.9.3, 1.11.1

[medium] CVE-2026-25542 — github.com/tektoncd/pipeline@v0.68.0

github.com/tektoncd/pipeline: Tekton Pipelines: Security bypass due to regular expression matching flaw

Fixed in: 1.0.2, 1.3.4, 1.6.2, 1.9.3, 1.11.1

[medium] CVE-2026-25680 — golang.org/x/net@v0.33.0

golang.org/x/net/html: golang.org/x/net/html: Denial of Service due to excessive HTML parsing

Fixed in: 0.55.0

[medium] CVE-2026-25680 — golang.org/x/net@v0.34.0

golang.org/x/net/html: golang.org/x/net/html: Denial of Service due to excessive HTML parsing

Fixed in: 0.55.0

[medium] CVE-2026-25680 — golang.org/x/net@v0.35.0

golang.org/x/net/html: golang.org/x/net/html: Denial of Service due to excessive HTML parsing

Fixed in: 0.55.0

[medium] CVE-2026-25680 — golang.org/x/net@v0.41.0

golang.org/x/net/html: golang.org/x/net/html: Denial of Service due to excessive HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-25680 — golang.org/x/net@v0.52.0

golang.org/x/net/html: golang.org/x/net/html: Denial of Service due to excessive HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-25934 — github.com/go-git/go-git/v5@v5.11.0

go-git/go-git: go-git: Data integrity issue due to improper verification of pack and index files
Fixed in: 5.16.5

[medium] CVE-2026-25934 — github.com/go-git/go-git/v5@v5.13.2

go-git/go-git: go-git: Data integrity issue due to improper verification of pack and index files
Fixed in: 5.16.5

[medium] CVE-2026-27142 — stdlib@1.22.12

html/template: URLs in meta content attribute actions are not escaped in html/template
Fixed in: 1.25.8, 1.26.1

[medium] CVE-2026-27142 — stdlib@1.23.6

html/template: URLs in meta content attribute actions are not escaped in html/template
Fixed in: 1.25.8, 1.26.1

[medium] CVE-2026-27142 — stdlib@1.25.5

html/template: URLs in meta content attribute actions are not escaped in html/template
Fixed in: 1.25.8, 1.26.1

[medium] CVE-2026-32282 — stdlib@1.22.12

golang: internal/syscall/unix: Root.Chmod can follow symlinks out of the root
Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32282 — stdlib@1.23.6

golang: internal/syscall/unix: Root.Chmod can follow symlinks out of the root
Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32282 — stdlib@1.25.5

golang: internal/syscall/unix: Root.Chmod can follow symlinks out of the root
Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32288 — stdlib@1.22.12

archive/tar: golang: Go's archive/tar package: Denial of Service via maliciously-crafted archive
Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32288 — stdlib@1.23.6

archive/tar: golang: Go's archive/tar package: Denial of Service via maliciously-crafted archive
Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32288 — stdlib@1.25.5

archive/tar: golang: Go's archive/tar package: Denial of Service via maliciously-crafted archive

Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32289 — stdlib@1.22.12

html/template: golang: html/template: Cross-Site Scripting (XSS) via improper context and brace depth tracking in JS template literals

Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32289 — stdlib@1.23.6

html/template: golang: html/template: Cross-Site Scripting (XSS) via improper context and brace depth tracking in JS template literals

Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32289 — stdlib@1.25.5

html/template: golang: html/template: Cross-Site Scripting (XSS) via improper context and brace depth tracking in JS template literals

Fixed in: 1.25.9, 1.26.2

[medium] CVE-2026-32952 — github.com/Azure/go-ntlmssp@v0.0.0-20211209120228-48547f28849e

go-ntlmssp: go-ntlmssp: Denial of Service via malicious NTLM challenge

Fixed in: 0.1.1

[medium] CVE-2026-33022 — github.com/tektoncd/pipeline@v0.65.1

github.com/tektoncd/pipeline: Tekton Pipelines: Denial of Service via long resolver names

Fixed in: 1.0.1, 1.3.3, 1.6.1, 1.9.2, 1.10.2

[medium] CVE-2026-33022 — github.com/tektoncd/pipeline@v0.68.0

github.com/tektoncd/pipeline: Tekton Pipelines: Denial of Service via long resolver names

Fixed in: 1.0.1, 1.3.3, 1.6.1, 1.9.2, 1.10.2

[medium] CVE-2026-33997 — github.com/docker/docker@v25.0.6+incompatible

moby: docker: github.com/moby/moby: Moby: Privilege validation bypass during plugin installation

Fixed in: 29.3.1

[medium] CVE-2026-33997 — github.com/docker/docker@v27.4.1+incompatible

moby: docker: github.com/moby/moby: Moby: Privilege validation bypass during plugin installation

Fixed in: 29.3.1

[medium] CVE-2026-33997 — github.com/docker/docker@v28.0.0+incompatible

moby: docker: github.com/moby/moby: Moby: Privilege validation bypass during plugin installation

Fixed in: 29.3.1

[medium] CVE-2026-34165 — github.com/go-git/go-git/v5@v5.11.0

github.com/go-git/go-git/v5: go-git: Denial of Service via crafted .idx file

Fixed in: 5.17.1

[medium] CVE-2026-34165 — github.com/go-git/go-git/v5@v5.13.2

github.com/go-git/go-git/v5: go-git: Denial of Service via crafted .idx file

Fixed in: 5.17.1

[medium] CVE-2026-39823 — stdlib@1.22.12

html/template: golang: Go html/template: Cross-Site Scripting via improper URL escaping in meta tag content

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39823 — stdlib@1.23.6

html/template: golang: Go html/template: Cross-Site Scripting via improper URL escaping in meta tag content

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39823 — stdlib@1.25.5

html/template: golang: Go html/template: Cross-Site Scripting via improper URL escaping in meta tag content

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39823 — stdlib@1.25.9

html/template: golang: Go html/template: Cross-Site Scripting via improper URL escaping in meta tag content

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39823 — stdlib@1.26.2

html/template: golang: Go html/template: Cross-Site Scripting via improper URL escaping in meta tag content

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39825 — stdlib@1.22.12

net/http/httputil: golang: net/http/httputil: ReverseProxy forwards hidden query parameters, potentially bypassing security controls

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39825 — stdlib@1.23.6

net/http/httputil: golang: net/http/httputil: ReverseProxy forwards hidden query parameters, potentially bypassing security controls

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39825 — stdlib@1.25.5

net/http/httputil: golang: net/http/httputil: ReverseProxy forwards hidden query parameters, potentially bypassing security controls

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39825 — stdlib@1.25.9

net/http/httputil: golang: net/http/httputil: ReverseProxy forwards hidden query parameters, potentially bypassing security controls

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39825 — stdlib@1.26.2

net/http/httputil: golang: net/http/httputil: ReverseProxy forwards hidden query parameters, potentially bypassing security controls

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39826 — stdlib@1.22.12

html/template: golang: html/template: Cross-site scripting due to incorrect script tag escaping

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39826 — stdlib@1.23.6

html/template: golang: html/template: Cross-site scripting due to incorrect script tag escaping

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39826 — stdlib@1.25.5

html/template: golang: html/template: Cross-site scripting due to incorrect script tag escaping

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39826 — stdlib@1.25.9

html/template: golang: html/template: Cross-site scripting due to incorrect script tag escaping

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39826 — stdlib@1.26.2

html/template: golang: html/template: Cross-site scripting due to incorrect script tag escaping

Fixed in: 1.25.10, 1.26.3

[medium] CVE-2026-39827 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via repeated rejected channel openings

Fixed in: 0.52.0

[medium] CVE-2026-39827 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via repeated rejected channel openings

Fixed in: 0.52.0

[medium] CVE-2026-39827 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via repeated rejected channel openings

Fixed in: 0.52.0

[medium] CVE-2026-39827 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service via repeated rejected channel openings

Fixed in: 0.52.0

[medium] CVE-2026-39833 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to unenforced key confirmation

Fixed in: 0.52.0

[medium] CVE-2026-39833 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to unenforced key confirmation

Fixed in: 0.52.0

[medium] CVE-2026-39833 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to unenforced key confirmation

Fixed in: 0.52.0

[medium] CVE-2026-39833 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh/agent: golang.org/x/crypto/ssh/agent: Security bypass due to unenforced key confirmation

Fixed in: 0.52.0

[medium] CVE-2026-39834 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service due to integer overflow in SSH channel write

Fixed in: 0.52.0

[medium] CVE-2026-39834 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service due to integer overflow in SSH channel write

Fixed in: 0.52.0

[medium] CVE-2026-39834 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service due to integer overflow in SSH channel write

Fixed in: 0.52.0

[medium] CVE-2026-39834 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh: golang: golang.org/x/crypto/ssh: Denial of Service due to integer overflow in SSH channel write

Fixed in: 0.52.0

[medium] CVE-2026-41506 — github.com/go-git/go-git/v5@v5.11.0

golang: github.com/go-git/go-git: go-git: Information disclosure of HTTP authentication credentials via redirects

Fixed in: 5.18.0

[medium] CVE-2026-41506 — github.com/go-git/go-git/v5@v5.13.2

golang: github.com/go-git/go-git: go-git: Information disclosure of HTTP authentication credentials via redirects

Fixed in: 5.18.0

[medium] CVE-2026-41568 — github.com/docker/docker@v25.0.6+incompatible

github.com/docker/docker: github.com/moby/moby: Moby: Denial of Service via race condition in docker cp mount setup

[medium] CVE-2026-41568 — github.com/docker/docker@v27.4.1+incompatible

github.com/docker/docker: github.com/moby/moby: Moby: Denial of Service via race condition in docker cp mount setup

[medium] CVE-2026-41568 — github.com/docker/docker@v28.0.0+incompatible

github.com/docker/docker: github.com/moby/moby: Moby: Denial of Service via race condition in

docker cp mount setup

[medium] CVE-2026-41579 — github.com/opencontainers/runc@v1.1.12

runc: runc: Host filesystem integrity compromised by malicious container images

Fixed in: 1.3.6, 1.4.3, 1.5.0-rc.3

[medium] CVE-2026-41888 — github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

github.com/distribution/distribution: Distribution: Security bypass allows unauthorized tag deletion

Fixed in: 3.1.1

[medium] CVE-2026-42502 — golang.org/x/net@v0.33.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via unexpected HTML tree rendering

Fixed in: 0.55.0

[medium] CVE-2026-42502 — golang.org/x/net@v0.34.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via unexpected HTML tree rendering

Fixed in: 0.55.0

[medium] CVE-2026-42502 — golang.org/x/net@v0.35.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via unexpected HTML tree rendering

Fixed in: 0.55.0

[medium] CVE-2026-42502 — golang.org/x/net@v0.41.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via unexpected HTML tree rendering

Fixed in: 0.55.0

[medium] CVE-2026-42502 — golang.org/x/net@v0.52.0

golang.org/x/net/html: golang: golang.org/x/net/html: Cross-Site Scripting via unexpected HTML tree rendering

Fixed in: 0.55.0

[medium] CVE-2026-42505 — stdlib@1.22.12

crypto/tls: golang: Go crypto/tls: Information disclosure in Encrypted Client Hello

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[medium] CVE-2026-42505 — stdlib@1.23.6

crypto/tls: golang: Go crypto/tls: Information disclosure in Encrypted Client Hello

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[medium] CVE-2026-42505 — stdlib@1.25.5

crypto/tls: golang: Go crypto/tls: Information disclosure in Encrypted Client Hello

Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[medium] CVE-2026-42505 — stdlib@1.25.9

crypto/tls: golang: Go crypto/tls: Information disclosure in Encrypted Client Hello
Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[medium] CVE-2026-42505 — stdlib@1.26.2

crypto/tls: golang: Go crypto/tls: Information disclosure in Encrypted Client Hello
Fixed in: 1.25.12, 1.26.5, 1.27.0-rc.2

[medium] CVE-2026-42506 — golang.org/x/net@v0.33.0

golang.org/x/net/html: golang.org/x/net/html: Cross-Site Scripting (XSS) via arbitrary HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-42506 — golang.org/x/net@v0.34.0

golang.org/x/net/html: golang.org/x/net/html: Cross-Site Scripting (XSS) via arbitrary HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-42506 — golang.org/x/net@v0.35.0

golang.org/x/net/html: golang.org/x/net/html: Cross-Site Scripting (XSS) via arbitrary HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-42506 — golang.org/x/net@v0.41.0

golang.org/x/net/html: golang.org/x/net/html: Cross-Site Scripting (XSS) via arbitrary HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-42506 — golang.org/x/net@v0.52.0

golang.org/x/net/html: golang.org/x/net/html: Cross-Site Scripting (XSS) via arbitrary HTML parsing
Fixed in: 0.55.0

[medium] CVE-2026-42507 — stdlib@1.22.12

net/textproto: golang: Golang net/textproto: Misleading error messages via input injection
Fixed in: 1.25.11, 1.26.4

[medium] CVE-2026-42507 — stdlib@1.23.6

net/textproto: golang: Golang net/textproto: Misleading error messages via input injection
Fixed in: 1.25.11, 1.26.4

[medium] CVE-2026-42507 — stdlib@1.25.5

net/textproto: golang: Golang net/textproto: Misleading error messages via input injection
Fixed in: 1.25.11, 1.26.4

[medium] CVE-2026-42507 — stdlib@1.25.9

net/textproto: golang: Golang net/textproto: Misleading error messages via input injection
Fixed in: 1.25.11, 1.26.4

[medium] CVE-2026-42507 — stdlib@1.26.2

net/textproto: golang: Golang net/textproto: Misleading error messages via input injection
Fixed in: 1.25.11, 1.26.4

[medium] CVE-2026-44740 — github.com/go-git/go-billy/v5@v5.5.0

github.com/go-git/go-billy: Billy: Denial of Service via crafted input due to insufficient validation

Fixed in: 5.9.0

[medium] CVE-2026-44740 — github.com/go-git/go-billy/v5@v5.6.2

github.com/go-git/go-billy: Billy: Denial of Service via crafted input due to insufficient validation

Fixed in: 5.9.0

[medium] CVE-2026-45571 — github.com/go-git/go-git/v5@v5.11.0

github.com/go-git/go-git: go-git: Path validation flaw allows unauthorized file access

Fixed in: 5.19.1

[medium] CVE-2026-45571 — github.com/go-git/go-git/v5@v5.13.2

github.com/go-git/go-git: go-git: Path validation flaw allows unauthorized file access

Fixed in: 5.19.1

[medium] CVE-2026-46598 — golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent: golang: golang.org/x/crypto/ssh/agent: Denial of Service via malformed input

Fixed in: 0.52.0

[medium] CVE-2026-46598 — golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent: golang: golang.org/x/crypto/ssh/agent: Denial of Service via malformed input

Fixed in: 0.52.0

[medium] CVE-2026-46598 — golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent: golang: golang.org/x/crypto/ssh/agent: Denial of Service via malformed input

Fixed in: 0.52.0

[medium] CVE-2026-46598 — golang.org/x/crypto@v0.49.0

golang.org/x/crypto/ssh/agent: golang: golang.org/x/crypto/ssh/agent: Denial of Service via malformed input

Fixed in: 0.52.0

[medium] CVE-2026-47262 — github.com/containerd/containerd@v1.7.11

github.com/containerd/containerd: containerd: Denial of Service via maliciously crafted image leading to unbounded group parsing

Fixed in: 1.7.33

[medium] CVE-2026-47262 — github.com/containerd/containerd@v1.7.32

github.com/containerd/containerd: containerd: Denial of Service via maliciously crafted image leading to unbounded group parsing

Fixed in: 1.7.33

[medium] CVE-2026-49834 — github.com/sigstore/sigstore-go@v0.7.0

github.com/sigstore/sigstore-go: sigstore-go: Security Policy Bypass via Compromised Log

Fixed in: 1.2.0

[medium] CVE-2026-49835 — github.com/sigstore/timestamp-authority@v1.2.4

timestamp-authority: Sigstore Timestamp Authority: Denial of Service via unbounded metric label

cardinality

[medium] CVE-2026-54168 — github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

Fixed in: 0.37.8, 0.39.6, 0.42.1, 0.48.0

[medium] CVE-2026-54168 — github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

Fixed in: 0.37.8, 0.39.6, 0.42.1, 0.48.0

[medium] CVE-2026-61711 — github.com/moby/buildkit@v0.12.5

BuildKit: Custom frontend could bypass Seccomp/AppArmor

Fixed in: 0.31.1

[medium] CVE-2026-61711 — github.com/moby/buildkit@v0.16.0

BuildKit: Custom frontend could bypass Seccomp/AppArmor

Fixed in: 0.31.1

[medium] CVE-2026-71557 — github.com/go-git/go-git/v5@v5.11.0

go-git is an extensible git implementation library written in pure Go. ...

Fixed in: 5.19.2

[medium] CVE-2026-71557 — github.com/go-git/go-git/v5@v5.13.2

go-git is an extensible git implementation library written in pure Go. ...

Fixed in: 5.19.2

[medium] GHSA-gcjh-h69q-9w9g — github.com/google/cel-go@v0.23.2

cel-go: JSON Private Fields Exposed via NativeTypes and ParseStructTag

Fixed in: 0.29.0

[medium] GHSA-pmwq-pjrm-6p5r — github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior

Fixed in: 0.11.0

[medium] GHSA-vrw8-fxc6-2r93 — github.com/go-chi/chi/v5@v5.1.0

chi Allows Host Header Injection which Leads to Open Redirect in RedirectSlashes

Fixed in: 5.2.2

[medium] GHSA-w5pp-99ch-qj29 — github.com/go-git/go-git/v5@v5.11.0

go-git: Malformed Git object data may cause panics or resource exhaustion

Fixed in: 5.19.1

[medium] GHSA-w5pp-99ch-qj29 — github.com/go-git/go-git/v5@v5.13.2

go-git: Malformed Git object data may cause panics or resource exhaustion

Fixed in: 5.19.1

[medium] GHSA-xmrv-pmrh-hhx2 — github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream@v1.6.8

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

Fixed in: 1.7.8

[medium] GHSA-xmrv-pmrh-hhx2 — github.com/aws/aws-sdk-go-v2/service/s3@v1.76.0

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

Fixed in: 1.97.3

[low] CVE-2025-54410 — github.com/docker/docker@v25.0.6+incompatible

github.com/moby/moby: Moby's Firewalld reload removes bridge network isolation

Fixed in: 25.0.13, 28.0.0

[low] CVE-2025-54410 — github.com/docker/docker@v27.4.1+incompatible

github.com/moby/moby: Moby's Firewalld reload removes bridge network isolation

Fixed in: 25.0.13, 28.0.0

[low] CVE-2025-58186 — stdlib@1.22.12

golang.org/net/http: Lack of limit when parsing cookies can cause memory exhaustion in net/http

Fixed in: 1.24.8, 1.25.2

[low] CVE-2025-58186 — stdlib@1.23.6

golang.org/net/http: Lack of limit when parsing cookies can cause memory exhaustion in net/http

Fixed in: 1.24.8, 1.25.2

[low] CVE-2025-8556 — github.com/cloudflare/circl@v1.3.7

github.com/cloudflare/circl: CIRCL-Fourq: Missing and wrong validation can lead to incorrect results

Fixed in: 1.6.1

[low] CVE-2026-1229 — github.com/cloudflare/circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[low] CVE-2026-1229 — github.com/cloudflare/circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[low] CVE-2026-27139 — stdlib@1.22.12

os: FileInfo can escape from a Root in golang os module

Fixed in: 1.25.8, 1.26.1

[low] CVE-2026-27139 — stdlib@1.23.6

os: FileInfo can escape from a Root in golang os module

Fixed in: 1.25.8, 1.26.1

[low] CVE-2026-27139 — stdlib@1.25.5

os: FileInfo can escape from a Root in golang os module

Fixed in: 1.25.8, 1.26.1

[low] CVE-2026-33762 — github.com/go-git/go-git/v5@v5.11.0

github.com/go-git/go-git/v5: go-git: Denial of Service via crafted Git index file

Fixed in: 5.17.1

[low] CVE-2026-33762 — github.com/go-git/go-git/v5@v5.13.2

github.com/go-git/go-git/v5: go-git: Denial of Service via crafted Git index file

Fixed in: 5.17.1

[low] CVE-2026-45570 — github.com/go-git/go-git/v5@v5.11.0

go-git is an extensible git implementation library written in pure Go. ...

Fixed in: 5.19.1

[low] CVE-2026-45570 — github.com/go-git/go-git/v5@v5.13.2

go-git is an extensible git implementation library written in pure Go. ...

Fixed in: 5.19.1

[low] CVE-2026-54787 — github.com/sigstore/sigstore-go@v0.7.0

github.com/sigstore/sigstore-go: sigstore-go: Signature bypass allows acceptance of bundles signed with expired keys

Fixed in: 1.2.1

[low] CVE-2026-61712 — github.com/moby/buildkit@v0.12.5

BuildKit has a possible runtime DoS via unbounded group parsing

Fixed in: 0.31.1

[low] CVE-2026-61712 — github.com/moby/buildkit@v0.16.0

BuildKit has a possible runtime DoS via unbounded group parsing

Fixed in: 0.31.1

[unknown] CVE-2026-39824 — golang.org/x/sys@v0.29.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

Fixed in: 0.44.0

[unknown] CVE-2026-39824 — golang.org/x/sys@v0.30.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

Fixed in: 0.44.0

[unknown] CVE-2026-39824 — golang.org/x/sys@v0.33.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

Fixed in: 0.44.0

[unknown] CVE-2026-39824 — golang.org/x/sys@v0.42.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

Fixed in: 0.44.0

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.32.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security

issues

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.33.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.39.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.49.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.53.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

Findings from osv-scanner

[unknown] GHSA-25mh-hp8x-cgrv (CVE-2025-14525) — kubevirt@UNKNOWN

KubeVirt Guest Agent DoS via Excessive Network Interface Reports

[unknown] GHSA-265r-hfxg-fhmg (CVE-2024-40635) — containerd@v1.7.11

containerd has an integer overflow in User ID handling

[unknown] GHSA-273p-m2cw-6833 (CVE-2026-23831) — rekor@v1.2.2

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

[unknown] GHSA-273p-m2cw-6833 (CVE-2026-23831) — rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

[unknown] GHSA-2r4r-5x78-mvqf (CVE-2025-64437) — kubevirt@UNKNOWN

KubeVirt Isolation Detection Flaw Allows Arbitrary File Permission Changes

[unknown] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — grpc@v1.67.1

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[unknown] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — grpc@v1.69.4

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[unknown] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — grpc@v1.70.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[unknown] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — grpc@v1.79.3

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[unknown] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — grpc@v1.80.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[unknown] GHSA-2x5j-vhc8-9cwm (CVE-2025-8556) — circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results

[unknown] GHSA-37cx-329c-33x3 (CVE-2026-25934) — v5@v5.11.0

go-git improperly verifies data integrity values for .idx and .pack files

[unknown] GHSA-37cx-329c-33x3 (CVE-2026-25934) — v5@v5.13.2

go-git improperly verifies data integrity values for .idx and .pack files

[unknown] GHSA-389r-gv7p-r3rp (CVE-2026-45022) — v5@v5.11.0

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

[unknown] GHSA-389r-gv7p-r3rp (CVE-2026-45022) — v5@v5.13.2

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

[unknown] GHSA-38jw-g2qx-4286 (CVE-2025-64432) — kubevirt@UNKNOWN

KubeVirt Affected by an Authentication Bypass in Kubernetes Aggregation Layer

[unknown] GHSA-3p65-76g6-3w7r (CVE-2026-33540) — v3@v3.0.0-20230519140516-983358f8e250

Distribution affected by pull-through cache credential exfiltration via www-authenticate bearer realm

[unknown] GHSA-3xc5-wrhm-f963 (CVE-2026-41506) — v5@v5.11.0

go-git: Credential leak via cross-host redirect in smart HTTP transport

[unknown] GHSA-3xc5-wrhm-f963 (CVE-2026-41506) — v5@v5.13.2

go-git: Credential leak via cross-host redirect in smart HTTP transport

[unknown] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — crypto@v0.32.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[unknown] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — crypto@v0.33.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[unknown] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — crypto@v0.39.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[unknown] GHSA-45gg-vh54-h5m9 (CVE-2026-39828) — crypto@v0.49.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[unknown] GHSA-46xp-26xh-hpqh (CVE-2025-64324) — kubevirt@UNKNOWN

KubeVirt Vulnerable to Arbitrary Host File Read and Write

[unknown] GHSA-47q9-m4ww-924m (CVE-2026-48702) — rekor@v1.2.2

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

[unknown] GHSA-47q9-m4ww-924m (CVE-2026-48702) — rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

[unknown] GHSA-4c29-8rgm-jvjj (CVE-2026-33747) — buildkit@v0.12.5

BuildKit's Malicious frontend can cause file escape outside of storage root

[unknown] GHSA-4c29-8rgm-jvjj (CVE-2026-33747) — buildkit@v0.16.0

BuildKit's Malicious frontend can cause file escape outside of storage root

[unknown] GHSA-4c4x-jm2x-pf9j (CVE-2026-24117) — rekor@v1.2.2

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

[unknown] GHSA-4c4x-jm2x-pf9j (CVE-2026-24117) — rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

[unknown] GHSA-4hfp-h4cw-hj8p (CVE-2025-32386) — v3@UNKNOWN

Helm Allows A Specially Crafted Chart Archive To Cause Out Of Memory Termination

[unknown] GHSA-4q63-mr2m-57hf (CVE-2024-33394) — kubevirt@UNKNOWN

kubevirt allows a local attacker to execute arbitrary code via a crafted command

[unknown] GHSA-4qg8-fj49-pxjh (CVE-2025-66564) — timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing

[unknown] GHSA-4vq8-7jfc-9cvp (CVE-2025-54410) — docker@v25.0.6+incompatible

Moby firewalld reload removes bridge network isolation

[unknown] GHSA-4vq8-7jfc-9cvp (CVE-2025-54410) — docker@v27.4.1+incompatible

Moby firewalld reload removes bridge network isolation

[unknown] GHSA-4vrq-3vrq-g6gg (CVE-2026-33748) — buildkit@v0.12.5

BuildKit Git URL subdir component can cause access to restricted files

[unknown] GHSA-4vrq-3vrq-g6gg (CVE-2026-33748) — buildkit@v0.16.0

BuildKit Git URL subdir component can cause access to restricted files

[unknown] GHSA-53c4-hhmh-vw5q (CVE-2022-23525) — v3@UNKNOWN

Helm vulnerable to denial of service through through repository index file

[unknown] GHSA-557j-xg8c-q2mm (CVE-2025-53547) — v3@UNKNOWN

Helm vulnerable to Code Injection through malicious chart.yaml content

[unknown] GHSA-56hp-xqp3-w2jf (CVE-2021-32690) — v3@UNKNOWN

Helm passes repository credentials to alternate domain

[unknown] GHSA-59jp-pj84-45mr (CVE-2026-22772) — fulcio@v1.4.3

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

[unknown] GHSA-59jp-pj84-45mr (CVE-2026-22772) — fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

[unknown] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — crypto@v0.32.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[unknown] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — crypto@v0.33.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[unknown] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — crypto@v0.39.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[unknown] GHSA-5cgq-3rg8-m6cv (CVE-2026-42508) — crypto@v0.49.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[unknown] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — net@v0.33.0

Go Net HTML parser is vulnerable to denial of service

[unknown] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — net@v0.34.0

Go Net HTML parser is vulnerable to denial of service

[unknown] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — net@v0.35.0

Go Net HTML parser is vulnerable to denial of service

[unknown] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — net@v0.41.0

Go Net HTML parser is vulnerable to denial of service

[unknown] GHSA-5cv4-jp36-h3mw (CVE-2026-25680) — net@v0.52.0

Go Net HTML parser is vulnerable to denial of service

[unknown] GHSA-5xqw-8hwv-wg92 (CVE-2025-32387) — v3@UNKNOWN

Helm Allows A Specially Crafted JSON Schema To Cause A Stack Overflow

[unknown] GHSA-67fx-wx78-jx33 (CVE-2022-23526) — v3@UNKNOWN

Helm vulnerable to denial of service through schema file

[unknown] GHSA-6f2p-296r-cc28 (CVE-2026-54168) — pipelines-as-code@v0.31.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

[unknown] GHSA-6f2p-296r-cc28 (CVE-2026-54168) — pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

[unknown] GHSA-6pjf-3r9x-m592 (CVE-2026-41888) — v3@v3.0.0-20230519140516-983358f8e250

Distribution's tag deletion bypasses `storage.delete.enabled` configuration

[unknown] GHSA-6rx9-889q-vv2r (CVE-2022-23524) — v3@UNKNOWN

Helm vulnerable to denial of service through string value parsing

[unknown] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — oauth2@v0.12.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[unknown] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — oauth2@v0.18.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[unknown] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — oauth2@v0.23.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[unknown] GHSA-6v2p-p543-phr9 (CVE-2025-22868) — oauth2@v0.26.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[unknown] GHSA-6wxm-mpqj-6jpf (CVE-2024-45339) — glog@UNKNOWN

Insecure Temporary File usage in github.com/golang/glog

[unknown] GHSA-6wxm-mpqj-6jpf (CVE-2024-45339) — glog@v1.2.2

Insecure Temporary File usage in github.com/golang/glog

[unknown] GHSA-7236-3392-c5c6 (CVE-2026-61711) — buildkit@v0.12.5

BuildKit: Custom frontend could bypass Seccomp/AppArmor

[unknown] GHSA-7236-3392-c5c6 (CVE-2026-61711) — buildkit@v0.16.0

BuildKit: Custom frontend could bypass Seccomp/AppArmor

[unknown] GHSA-72x6-4j93-7w86 (CVE-2026-61712) — buildkit@v0.12.5

BuildKit has a possible runtime DoS via unbounded group parsing

[unknown] GHSA-72x6-4j93-7w86 (CVE-2026-61712) — buildkit@v0.16.0

BuildKit has a possible runtime DoS via unbounded group parsing

[unknown] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — v3@v3.0.3

Go JOSE Panics in JWE decryption

[unknown] GHSA-78h2-9frx-2jm8 (CVE-2026-34986) — v4@v4.0.5

Go JOSE Panics in JWE decryption

[unknown] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — crypto@v0.32.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[unknown] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — crypto@v0.33.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[unknown] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — crypto@v0.39.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[unknown] GHSA-78mq-xcr3-xm33 (CVE-2026-39835) — crypto@v0.49.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[unknown] GHSA-7hfp-qfw3-5jxh (CVE-2022-36055) — v3@UNKNOWN

Helm Vulnerable to denial of service through string value parsing

[unknown] GHSA-7jcp-v9w4-wjmg (CVE-2026-7374) — kubevirt@UNKNOWN

KubeVirt has a Link Following vulnerability

[unknown] GHSA-7jxh-36q5-gcqv (CVE-2026-53495) — containerd@v1.7.11

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service

[unknown] GHSA-7jxh-36q5-gcqv (CVE-2026-53495) — containerd@v1.7.32

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service

[unknown] GHSA-7xgm-5prm-v5gc (CVE-2025-64436) — kubevirt@UNKNOWN

KubeVirt Excessive Role Permissions Could Enable Unauthorized VMI Migrations Between Nodes

[unknown] GHSA-828r-r2c8-rfw3 (CVE-2020-14316) — kubevirt@UNKNOWN

Privilege Escalation in kubevirt

[unknown] GHSA-846p-jg2w-w324 (CVE-2026-23991) — v2@v2.0.2

go-tuf affected by client DoS via malformed server response

[unknown] GHSA-849r-8wvp-4wwg (CVE-2020-1701) — kubevirt@UNKNOWN

Permissions bypass in KubeVirt

[unknown] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — crypto@v0.32.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[unknown] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — crypto@v0.33.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[unknown] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — crypto@v0.39.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[unknown] GHSA-89gr-r52h-f8rx (CVE-2026-39831) — crypto@v0.49.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[unknown] GHSA-89xv-2j6f-qhc8 (CVE-2026-33252) — go-sdk@v1.1.0

Cross-Site Tool Execution for HTTP Servers without Authorizatrion in github.com/modelcontextprotocol/go-sdk

[unknown] GHSA-8wmf-6v46-5gfg (CVE-2026-81870) — sdk@v1.34.0

OpenTelemetry-Go: Exporter config logging may leak endpoint URLs in info logs

[unknown] GHSA-9493-h29p-rfm2 (CVE-2025-31133) — runc@v1.1.12

runc container escape via "masked path" abuse due to mount race conditions

[unknown] GHSA-9c54-x2g4-v92j (CVE-2026-49835) — timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality

[unknown] GHSA-9h84-qmv7-982p (CVE-2025-55199) — v3@UNKNOWN

Helm Charts with Specific JSON Schema Values Can Cause Memory Exhaustion

[unknown] GHSA-9h8m-3fm2-qjrq (CVE-2026-24051) — sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking

[unknown] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — crypto@v0.32.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[unknown] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — crypto@v0.33.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[unknown] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — crypto@v0.39.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[unknown] GHSA-9m57-25v3-79x9 (CVE-2026-46598) — crypto@v0.49.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[unknown] GHSA-9m94-w2vq-hcf9 (CVE-2025-64435) — kubevirt@UNKNOWN

KubeVirt VMI Denial-of-Service (DoS) Using Pod Impersonation

[unknown] GHSA-9vcr-p3rj-q5q6 (CVE-2026-49834) — sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log

[unknown] GHSA-c6gw-w398-hv78 (CVE-2025-27144) — v3@v3.0.3

DoS in go-jose Parsing

[unknown] GHSA-cgrx-mc8f-2prm (CVE-2025-52881) — runc@v1.1.12

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

[unknown] GHSA-cgrx-mc8f-2prm (CVE-2025-52881) — selinux@v1.11.0

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

[unknown] GHSA-cp6g-7hqx-qxhp (CVE-2026-2303) — mongo-driver@v1.14.0

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

[unknown] GHSA-cp6g-7hqx-qxhp (CVE-2026-2303) — mongo-driver@v1.16.1

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

[unknown] GHSA-cp96-jpmq-xrr2 (CVE-2023-26484) — kubevirt@UNKNOWN

On a compromised node, the virt-handler service account can be used to modify all node specs

[unknown] GHSA-crhj-59gh-8x96 (CVE-2026-45571) — v5@v5.11.0

go-git: Crafted repositories may modify main and submodule .git directories

[unknown] GHSA-crhj-59gh-8x96 (CVE-2026-45571) — v5@v5.13.2

go-git: Crafted repositories may modify main and submodule .git directories

[unknown] GHSA-cv4x-93xx-wgfj (CVE-2026-33022) — pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

[unknown] GHSA-cv4x-93xx-wgfj (CVE-2026-33022) — pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

[unknown] GHSA-f2g3-hh2r-cwgc (CVE-2026-35172) — v3@v3.0.0-20230519140516-983358f8e250

Distribution: stale blob access resurrection via repo-scoped redis descriptor cache invalidation

[unknown] GHSA-f5f4-3hh4-f54m (CVE-2026-54167) — pipelines-as-code@v0.31.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

[unknown] GHSA-f5f4-3hh4-f54m (CVE-2026-54167) — pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

[unknown] GHSA-f5mr-q85p-6hh6 (CVE-2026-49478) — fulcio@v1.4.3

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

[unknown] GHSA-f5mr-q85p-6hh6 (CVE-2026-49478) — fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

[unknown] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — crypto@v0.32.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[unknown] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — crypto@v0.33.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[unknown] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — crypto@v0.39.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[unknown] GHSA-f5wc-c3c7-36mc (CVE-2026-39832) — crypto@v0.49.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[unknown] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — crypto@v0.32.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

[unknown] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — crypto@v0.33.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

[unknown] GHSA-f6x5-jh6r-wrfv (CVE-2025-47914) — crypto@v0.39.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

[unknown] GHSA-f83f-xpx7-ffpw (CVE-2025-66506) — fulcio@v1.4.3

Fulcio allocates excessive memory during token parsing

[unknown] GHSA-f83f-xpx7-ffpw (CVE-2025-66506) — fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing

[unknown] GHSA-f9f8-9pmf-xv68 (CVE-2025-55198) — v3@UNKNOWN

Helm May Panic Due To Incorrect YAML Content

[unknown] GHSA-fcv2-xgw5-pqxf (CVE-2026-24137) — sigstore@v1.8.15

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

[unknown] GHSA-fcv2-xgw5-pqxf (CVE-2026-24137) — sigstore@v1.8.2

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

[unknown] GHSA-fphv-w9fq-2525 (CVE-2026-23992) — v2@v2.0.2

go-tuf improperly validates the configured threshold for delegations

[unknown] GHSA-fxhp-mv3v-67qp (CVE-2026-50163) — v2@v2.6.1

`oras-go` tar extraction: Hardlink entry with relative Linkname escapes extract dir via process CWD resolution

[unknown] GHSA-gcjh-h69q-9w9g — cel-go@v0.23.2

cel-go: JSON Private Fields Exposed via NativeTypes and ParseStructTag

[unknown] GHSA-ggp9-c99x-54gp (CVE-2025-64434) — kubevirt@UNKNOWN

KubeVirt's Improper TLS Certificate Management Handling Allows API Identity Spoofing

[unknown] GHSA-gm2x-2g9h-ccm8 (CVE-2026-33762) — v5@v5.11.0

go-git missing validation decoding Index v4 files leads to panic

[unknown] GHSA-gm2x-2g9h-ccm8 (CVE-2026-33762) — v5@v5.13.2

go-git missing validation decoding Index v4 files leads to panic

[unknown] GHSA-h7vf-4x9w-h99v (CVE-2026-85732) — v2@v2.6.1

oras-go: Blind SSRF via unvalidated Link header URL in pagination allows internal network probing

[unknown] GHSA-hc8v-wwc9-vgxm (CVE-2026-71556) — v5@v5.11.0

go-git: Worktree operations may follow symlinks

[unknown] GHSA-hc8v-wwc9-vgxm (CVE-2026-71556) — v5@v5.13.2

go-git: Worktree operations may follow symlinks

[unknown] GHSA-hcg3-q754-cr77 (CVE-2025-22869) — crypto@v0.32.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

[unknown] GHSA-hcg3-q754-cr77 (CVE-2025-22869) — crypto@v0.33.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

[unknown] GHSA-hfvc-g4fc-pqhx (CVE-2026-39883) — sdk@v1.34.0

opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking

[unknown] GHSA-hr2v-4r36-88hr (CVE-2026-35206) — v3@UNKNOWN

Helm Chart extraction output directory collapse via `Chart.yaml` name dot-segment

[unknown] GHSA-hrxh-6v49-42gf — grpc@v1.67.1

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[unknown] GHSA-hrxh-6v49-42gf — grpc@v1.69.4

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[unknown] GHSA-hrxh-6v49-42gf — grpc@v1.70.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[unknown] GHSA-hrxh-6v49-42gf — grpc@v1.79.3

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[unknown] GHSA-hrxh-6v49-42gf — grpc@v1.80.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[unknown] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — crypto@v0.32.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

[unknown] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — crypto@v0.33.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

[unknown] GHSA-j5w8-q4qc-rx2x (CVE-2025-58181) — crypto@v0.39.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

[unknown] GHSA-j6cv-3w8p-vrg8 (CVE-2026-6383) — kubevirt@UNKNOWN

KubeVirt's authorization mechanism improperly truncates subresource names

[unknown] GHSA-jc7w-c686-c4v9 (CVE-2025-58058) — xz@v0.5.11

github.com/ulikunitz/xz leaks memory when decoding a corrupted multiple LZMA archives

[unknown] GHSA-jfvp-7x6p-h2pv (CVE-2024-45310) — runc@v1.1.12

runc can be confused to create empty files/directories on the host

[unknown] GHSA-jhf3-xxhw-2wpp (CVE-2026-34165) — v5@v5.11.0

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

[unknown] GHSA-jhf3-xxhw-2wpp (CVE-2026-34165) — v5@v5.13.2

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

[unknown] GHSA-jpcc-p29g-p8mq (CVE-2026-47262) — containerd@v1.7.11

containerd image-triggered runtime DoS via unbounded group parsing

[unknown] GHSA-jpcc-p29g-p8mq (CVE-2026-47262) — containerd@v1.7.32

containerd image-triggered runtime DoS via unbounded group parsing

[unknown] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — crypto@v0.32.0

golang.org/x/crypto doesn't enforce invoking key constraints

[unknown] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — crypto@v0.33.0

golang.org/x/crypto doesn't enforce invoking key constraints

[unknown] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — crypto@v0.39.0

golang.org/x/crypto doesn't enforce invoking key constraints

[unknown] GHSA-jppx-rxg9-jmrx (CVE-2026-39833) — crypto@v0.49.0

golang.org/x/crypto doesn't enforce invoking key constraints

[unknown] GHSA-jqc5-w2xx-5vq4 (CVE-2026-24686) — v2@v2.0.2

go-tuf Path Traversal in TAP 4 Multirepo Client Allows Arbitrary File Write via Malicious Repository Names

[unknown] GHSA-m37j-52j7-pjw7 (CVE-2026-85731) — v2@v2.6.1

oras-go: Arbitrary file write outside file.Store root via symlink-chain bypass in tar extraction (pushDir)

[unknown] GHSA-m3xc-h892-ggx6 (CVE-2026-44740) — v5@v5.5.0

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

[unknown] GHSA-m3xc-h892-ggx6 (CVE-2026-44740) — v5@v5.6.2

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

[unknown] GHSA-m6hq-p25p-ffr2 (CVE-2025-64329) — containerd@v1.7.11

containerd CRI server: Host memory exhaustion through Attach goroutine leak

[unknown] GHSA-m7cr-m3pv-hgrp (CVE-2026-45570) — v5@v5.11.0

go-git: Improper single-quote escaping in go-git SSH transport

[unknown] GHSA-m7cr-m3pv-hgrp (CVE-2026-45570) — v5@v5.13.2

go-git: Improper single-quote escaping in go-git SSH transport

[unknown] GHSA-mh63-6h87-95cp (CVE-2025-30204) — v4@v4.5.1

jwt-go allows excessive memory allocation during header parsing

[unknown] GHSA-mh63-6h87-95cp (CVE-2025-30204) — v5@v5.2.1

jwt-go allows excessive memory allocation during header parsing

[unknown] GHSA-mpmf-3w4r-qfpf (CVE-2026-9804) — kubevirt@UNKNOWN

KubeVirt has a Link Following issue

[unknown] GHSA-p436-gjf2-799p (CVE-2025-15558) — cli@v27.4.1+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

[unknown] GHSA-p436-gjf2-799p (CVE-2025-15558) — cli@v28.0.0+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

[unknown] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — grpc@v1.67.1

gRPC-Go has an authorization bypass via missing leading slash in :path

[unknown] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — grpc@v1.69.4

gRPC-Go has an authorization bypass via missing leading slash in :path

[unknown] GHSA-p77j-4mvh-x3m3 (CVE-2026-33186) — grpc@v1.70.0

gRPC-Go has an authorization bypass via missing leading slash in :path

[unknown] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — spdystream@v0.2.0

SpdyStream: DOS on CRI

[unknown] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — spdystream@v0.4.0

SpdyStream: DOS on CRI

[unknown] GHSA-pc3f-x583-g7j2 (CVE-2026-35469) — spdystream@v0.5.0

SpdyStream: DOS on CRI

[unknown] GHSA-pmwq-pjrm-6p5r — in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior

[unknown] GHSA-pwhc-rpq9-4c8w (CVE-2024-25621) — containerd@v1.7.11

containerd affected by a local privilege escalation via wide permissions on CRI directory

[unknown] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — docker@v25.0.6+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[unknown] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — docker@v27.4.1+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[unknown] GHSA-pxq6-2prw-chj9 (CVE-2026-33997) — docker@v28.0.0+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[unknown] GHSA-q382-vc8q-7jhj — go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

[unknown] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — crypto@v0.32.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[unknown] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — crypto@v0.33.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[unknown] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — crypto@v0.39.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[unknown] GHSA-q4h4-gmj2-qvw2 (CVE-2026-46597) — crypto@v0.49.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[unknown] GHSA-q9hv-hpm4-hj6x (CVE-2026-1229) — circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult

[unknown] GHSA-q9hv-hpm4-hj6x (CVE-2026-1229) — circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult

[unknown] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — grpc@v1.67.1

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — grpc@v1.69.4

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — grpc@v1.70.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — grpc@v1.79.3

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — grpc@v1.80.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] GHSA-qgq7-7hm3-q39j (CVE-2026-71557) — v5@v5.11.0

go-git: Malicious reference names may modify files outside the reference storage

[unknown] GHSA-qgq7-7hm3-q39j (CVE-2026-71557) — v5@v5.13.2

go-git: Malicious reference names may modify files outside the reference storage

[unknown] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — crypto@v0.32.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[unknown] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — crypto@v0.33.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[unknown] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — crypto@v0.39.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[unknown] GHSA-qpw4-5x99-6vjp (CVE-2026-39827) — crypto@v0.49.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[unknown] GHSA-qw64-3x98-g7q2 (CVE-2026-44973) — v5@v5.5.0

go-billy has path traversal vulnerabilities

[unknown] GHSA-qw64-3x98-g7q2 (CVE-2026-44973) — v5@v5.6.2

go-billy has path traversal vulnerabilities

[unknown] GHSA-qw6q-3pgr-5cwq (CVE-2025-64433) — kubevirt@UNKNOWN

KubeVirt Arbitrary Container File Read

[unknown] GHSA-qw9x-cqr3-wc7r (CVE-2025-52565) — runc@v1.1.12

runc container escape with malicious config due to /dev/console mount and related races

[unknown] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — net@v0.34.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GHSA-qxp5-gwg8-xv66 (CVE-2025-22870) — net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GHSA-r53h-jv2g-vpx6 (CVE-2024-26147) — v3@UNKNOWN

Helm's Missing YAML Content Leads To Panic

[unknown] GHSA-r9px-m959-cxf4 (CVE-2025-21614) — v5@v5.11.0

go-git clients vulnerable to DoS via maliciously crafted Git server replies

[unknown] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — docker@v25.0.6+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[unknown] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — docker@v27.4.1+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[unknown] GHSA-rg2x-37c3-w2rh (CVE-2026-42306) — docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[unknown] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — crypto@v0.32.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[unknown] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — crypto@v0.33.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[unknown] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — crypto@v0.39.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[unknown] GHSA-rm3j-f69w-wqmq (CVE-2026-39834) — crypto@v0.49.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[unknown] GHSA-rmx9-2pp3-xhcr (CVE-2026-25542) — pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

[unknown] GHSA-rmx9-2pp3-xhcr (CVE-2026-25542) — pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

[unknown] GHSA-v53g-5gjp-272r (CVE-2024-25620) — v3@UNKNOWN

Helm dependency management path traversal

[unknown] GHSA-v725-9546-7q7m (CVE-2025-21613) — v5@v5.11.0

go-git has an Argument Injection via the URL field

[unknown] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — crypto@v0.32.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[unknown] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — crypto@v0.33.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[unknown] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — crypto@v0.39.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[unknown] GHSA-vgwf-h737-ff37 (CVE-2026-39830) — crypto@v0.49.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[unknown] GHSA-vjhf-6xfr-5p9g (CVE-2024-31420) — kubevirt@UNKNOWN

KubeVirt NULL pointer dereference flaw

[unknown] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — grpc@v1.67.1

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[unknown] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — grpc@v1.69.4

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[unknown] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — grpc@v1.70.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[unknown] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — grpc@v1.79.3

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[unknown] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — grpc@v1.80.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[unknown] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — docker@v25.0.6+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[unknown] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — docker@v27.4.1+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[unknown] GHSA-vp62-88p7-qqf5 (CVE-2026-41568) — docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[unknown] GHSA-vrw8-fxc6-2r93 (CVE-2025-71405) — v5@v5.1.0

chi Allows Host Header Injection which Leads to Open Redirect in RedirectSlashes

[unknown] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — net@v0.33.0

golang.org/x/net vulnerable to Cross-site Scripting

[unknown] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — net@v0.34.0

golang.org/x/net vulnerable to Cross-site Scripting

[unknown] GHSA-vvgc-356p-c3xw (CVE-2025-22872) — net@v0.35.0

golang.org/x/net vulnerable to Cross-site Scripting

[unknown] GHSA-w5pp-99ch-qj29 — v5@v5.11.0

go-git: Malformed Git object data may cause panics or resource exhaustion

[unknown] GHSA-w5pp-99ch-qj29 — v5@v5.13.2

go-git: Malformed Git object data may cause panics or resource exhaustion

[unknown] GHSA-w67g-5rqw-f597 — websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

[unknown] GHSA-w67g-5rqw-f597 — websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

[unknown] GHSA-w67g-5rqw-f597 — websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

[unknown] GHSA-w879-237q-wc7r (CVE-2026-39829) — crypto@v0.32.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[unknown] GHSA-w879-237q-wc7r (CVE-2026-39829) — crypto@v0.33.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[unknown] GHSA-w879-237q-wc7r (CVE-2026-39829) — crypto@v0.39.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[unknown] GHSA-w879-237q-wc7r (CVE-2026-39829) — crypto@v0.49.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[unknown] GHSA-whqx-f9j3-ch6m (CVE-2026-22703) — v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions

[unknown] GHSA-wqqc-jjcq-vfxm (CVE-2026-54787) — sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period

[unknown] GHSA-wvj2-96wp-fq3f (CVE-2026-27896) — go-sdk@v1.1.0

MCP Go SDK Vulnerable to Improper Handling of Case Sensitivity

[unknown] GHSA-x527-x647-q7gg (CVE-2026-46595) — crypto@v0.32.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[unknown] GHSA-x527-x647-q7gg (CVE-2026-46595) — crypto@v0.33.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[unknown] GHSA-x527-x647-q7gg (CVE-2026-46595) — crypto@v0.39.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[unknown] GHSA-x527-x647-q7gg (CVE-2026-46595) — crypto@v0.49.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[unknown] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — docker@v25.0.6+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[unknown] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — docker@v27.4.1+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[unknown] GHSA-x86f-5xw2-fm2r (CVE-2026-41567) — docker@v28.0.0+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[unknown] GHSA-xhf5-7wjv-pqxp (CVE-2026-53488) — containerd@v1.7.11

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

[unknown] GHSA-xhf5-7wjv-pqxp (CVE-2026-53488) — containerd@v1.7.32

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

[unknown] GHSA-xjvp-4fhw-gc47 (CVE-2026-41579) — runc@v1.1.12

runc: Malicious image with /dev symlink can trigger limited host filesystem integrity violations

[unknown] GHSA-xmrv-pmrh-hhx2 (CVE-2026-89090) — eventstream@v1.6.8

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

[unknown] GHSA-xmrv-pmrh-hhx2 (CVE-2026-89090) — s3@v1.76.0

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

[unknown] GHSA-xw59-hvm2-8pj6 (CVE-2026-34742) — go-sdk@v1.1.0

DNS Rebinding Protection Disabled by Default in Model Context Protocol Go SDK for Servers Running on Localhost

[unknown] GO-2022-0384 (CVE-2021-32690) — v3@UNKNOWN

Repository credentials passed to alternate domain in helm.sh/helm/v3

[unknown] GO-2022-0635 (CVE-2020-8912) — aws-sdk-go@v1.53.12

In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] GO-2022-0635 (CVE-2020-8912) — aws-sdk-go@v1.55.6

In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] GO-2022-0646 (CVE-2020-8911) — aws-sdk-go@v1.53.12

CBC padding oracle issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] GO-2022-0646 (CVE-2020-8911) — aws-sdk-go@v1.55.6

CBC padding oracle issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] GO-2022-0962 (CVE-2022-36055) — v3@UNKNOWN

Denial of service through string value parsing in helm.sh/helm/v3

[unknown] GO-2022-1165 (CVE-2022-23525) — v3@UNKNOWN

Denial of service via repository index file in helm.sh/helm/v3

[unknown] GO-2022-1166 (CVE-2022-23526) — v3@UNKNOWN

Denial of service via schema file in helm.sh/helm/v3

[unknown] GO-2022-1167 (CVE-2022-23524) — v3@UNKNOWN

Denial of service in string value parsing in helm.sh/helm/v3

[unknown] GO-2023-1547 (CVE-2023-25165) — v3@UNKNOWN

Information disclosure in helm.sh/helm/v3

[unknown] GO-2023-1901 (CVE-2023-37264) — pipeline@v0.65.1

Pipelines do not validate child UIDs in github.com/tektoncd/pipeline

[unknown] GO-2023-1901 (CVE-2023-37264) — pipeline@v0.68.0

Pipelines do not validate child UIDs in github.com/tektoncd/pipeline

[unknown] GO-2024-2554 (CVE-2024-25620) — v3@UNKNOWN

Path traversal in helm.sh/helm/v3

[unknown] GO-2024-2575 (CVE-2024-26147) — v3@UNKNOWN

Helm's Missing YAML Content Leads To Panic in helm.sh/helm/v3

[unknown] GO-2024-2688 (CVE-2024-31420) — kubevirt@UNKNOWN

KubeVirt NULL pointer dereference flaw in kubevirt.io/kubevirt

[unknown] GO-2024-2756 (CVE-2020-14316) — kubevirt@UNKNOWN

Privilege Escalation in kubevirt in kubevirt.io/kubevirt

[unknown] GO-2024-2765 (CVE-2020-1701) — kubevirt@UNKNOWN

Permissions bypass in KubeVirt in kubevirt.io/kubevirt

[unknown] GO-2024-2816 (CVE-2024-33394) — kubevirt@UNKNOWN

kubevirt allows a local attacker to execute arbitrary code via a crafted command in kubevirt.io/kubevirt

[unknown] GO-2024-2866 (CVE-2024-5042) — submariner-operator@v0.24.0

Submariner Operator sets unnecessary RBAC permissions in helm charts in github.com/submariner-io/submariner-operator

[unknown] GO-2024-3110 (CVE-2024-45310) — runc@v1.1.12

Can be confused to create empty files/directories on the host in github.com/opencontainers/runc

[unknown] GO-2025-3367 (CVE-2025-21614) — v5@v5.11.0

Clients vulnerable to DoS via maliciously crafted Git server replies in github.com/go-git/go-git

[unknown] GO-2025-3368 (CVE-2025-21613) — v5@v5.11.0

Argument Injection via the URL field in github.com/go-git/go-git

[unknown] GO-2025-3372 (CVE-2024-45339) — glog@UNKNOWN

Vulnerability when creating log files in github.com/golang/glog

[unknown] GO-2025-3372 (CVE-2024-45339) — glog@v1.2.2

Vulnerability when creating log files in github.com/golang/glog

[unknown] GO-2025-3485 (CVE-2025-27144) — v3@v3.0.3

DoS in go-jose Parsing in github.com/go-jose/go-jose

[unknown] GO-2025-3487 (CVE-2025-22869) — crypto@v0.32.0

Potential denial of service in golang.org/x/crypto

[unknown] GO-2025-3487 (CVE-2025-22869) — crypto@v0.33.0

Potential denial of service in golang.org/x/crypto

[unknown] GO-2025-3488 (CVE-2025-22868) — oauth2@v0.12.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] GO-2025-3488 (CVE-2025-22868) — oauth2@v0.18.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] GO-2025-3488 (CVE-2025-22868) — oauth2@v0.23.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] GO-2025-3488 (CVE-2025-22868) — oauth2@v0.26.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] GO-2025-3503 (CVE-2025-22870) — net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GO-2025-3503 (CVE-2025-22870) — net@v0.34.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GO-2025-3503 (CVE-2025-22870) — net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GO-2025-3503 (CVE-2025-22870) — stdlib@1.22.12

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GO-2025-3503 (CVE-2025-22870) — stdlib@1.23.6

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GO-2025-3528 (CVE-2024-40635) — containerd@v1.7.11

containerd has an integer overflow in User ID handling in github.com/containerd/containerd

[unknown] GO-2025-3553 (CVE-2025-30204) — v4@v4.5.1

Excessive memory allocation during header parsing in github.com/golang-jwt/jwt

[unknown] GO-2025-3553 (CVE-2025-30204) — v5@v5.2.1

Excessive memory allocation during header parsing in github.com/golang-jwt/jwt

[unknown] GO-2025-3563 (CVE-2025-22871) — stdlib@1.22.12

Request smuggling due to acceptance of invalid chunked data in net/http

[unknown] GO-2025-3563 (CVE-2025-22871) — stdlib@1.23.6

Request smuggling due to acceptance of invalid chunked data in net/http

[unknown] GO-2025-3595 (CVE-2025-22872) — net@v0.33.0

Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

[unknown] GO-2025-3595 (CVE-2025-22872) — net@v0.34.0

Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

[unknown] GO-2025-3595 (CVE-2025-22872) — net@v0.35.0

Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

[unknown] GO-2025-3601 (CVE-2025-32386) — v3@UNKNOWN

Helm Allows A Specially Crafted Chart Archive To Cause Out Of Memory Termination in helm.sh/helm

[unknown] GO-2025-3602 (CVE-2025-32387) — v3@UNKNOWN

Helm Allows A Specially Crafted JSON Schema To Cause A Stack Overflow in helm.sh/helm

[unknown] GO-2025-3750 (CVE-2025-0913) — stdlib@1.22.12

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

[unknown] GO-2025-3750 (CVE-2025-0913) — stdlib@1.23.6

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

[unknown] GO-2025-3751 (CVE-2025-4673) — stdlib@1.22.12

Sensitive headers not cleared on cross-origin redirect in net/http

[unknown] GO-2025-3751 (CVE-2025-4673) — stdlib@1.23.6

Sensitive headers not cleared on cross-origin redirect in net/http

[unknown] GO-2025-3754 (CVE-2025-8556) — circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results in github.com/cloudflare/circl

[unknown] GO-2025-3802 (CVE-2025-53547) — v3@UNKNOWN

Helm vulnerable to Code Injection through malicious chart.yaml content in helm.sh/helm

[unknown] GO-2025-3829 (CVE-2025-54410) — docker@v25.0.6+incompatible

Moby firewalld reload removes bridge network isolation in github.com/docker/docker

[unknown] GO-2025-3849 (CVE-2025-47907) — stdlib@1.22.12

Incorrect results returned from Rows.Scan in database/sql

[unknown] GO-2025-3849 (CVE-2025-47907) — stdlib@1.23.6

Incorrect results returned from Rows.Scan in database/sql

[unknown] GO-2025-3887 (CVE-2025-55199) — v3@UNKNOWN

Helm Charts with Specific JSON Schema Values Can Cause Memory Exhaustion in helm.sh/helm

[unknown] GO-2025-3888 (CVE-2025-55198) — v3@UNKNOWN

Helm May Panic Due To Incorrect YAML Content in helm.sh/helm

[unknown] GO-2025-3922 (CVE-2025-58058) — xz@v0.5.11

Memory leaks when decoding a corrupted multiple LZMA archives in github.com/ulikunitz/xz

[unknown] GO-2025-3956 (CVE-2025-47906) — stdlib@1.22.12

Unexpected paths returned from LookPath in os/exec

[unknown] GO-2025-3956 (CVE-2025-47906) — stdlib@1.23.6

Unexpected paths returned from LookPath in os/exec

[unknown] GO-2025-4006 (CVE-2025-61725) — stdlib@1.22.12

Excessive CPU consumption in ParseAddress in net/mail

[unknown] GO-2025-4006 (CVE-2025-61725) — stdlib@1.23.6

Excessive CPU consumption in ParseAddress in net/mail

[unknown] GO-2025-4007 (CVE-2025-58187) — stdlib@1.22.12

Quadratic complexity when checking name constraints in crypto/x509

[unknown] GO-2025-4007 (CVE-2025-58187) — stdlib@1.23.6

Quadratic complexity when checking name constraints in crypto/x509

[unknown] GO-2025-4008 (CVE-2025-58189) — stdlib@1.22.12

ALPN negotiation error contains attacker controlled information in crypto/tls

[unknown] GO-2025-4008 (CVE-2025-58189) — stdlib@1.23.6

ALPN negotiation error contains attacker controlled information in crypto/tls

[unknown] GO-2025-4009 (CVE-2025-61723) — stdlib@1.22.12

Quadratic complexity when parsing some invalid inputs in encoding/pem

[unknown] GO-2025-4009 (CVE-2025-61723) — stdlib@1.23.6

Quadratic complexity when parsing some invalid inputs in encoding/pem

[unknown] GO-2025-4010 (CVE-2025-47912) — stdlib@1.22.12

Insufficient validation of bracketed IPv6 hostnames in net/url

[unknown] GO-2025-4010 (CVE-2025-47912) — stdlib@1.23.6

Insufficient validation of bracketed IPv6 hostnames in net/url

[unknown] GO-2025-4011 (CVE-2025-58185) — stdlib@1.22.12

Parsing DER payload can cause memory exhaustion in encoding/asn1

[unknown] GO-2025-4011 (CVE-2025-58185) — stdlib@1.23.6

Parsing DER payload can cause memory exhaustion in encoding/asn1

[unknown] GO-2025-4012 (CVE-2025-58186) — stdlib@1.22.12

Lack of limit when parsing cookies can cause memory exhaustion in net/http

[unknown] GO-2025-4012 (CVE-2025-58186) — stdlib@1.23.6

Lack of limit when parsing cookies can cause memory exhaustion in net/http

[unknown] GO-2025-4013 (CVE-2025-58188) — stdlib@1.22.12

Panic when validating certificates with DSA public keys in crypto/x509

[unknown] GO-2025-4013 (CVE-2025-58188) — stdlib@1.23.6

Panic when validating certificates with DSA public keys in crypto/x509

[unknown] GO-2025-4014 (CVE-2025-58183) — stdlib@1.22.12

Unbounded allocation when parsing GNU sparse map in archive/tar

[unknown] GO-2025-4014 (CVE-2025-58183) — stdlib@1.23.6

Unbounded allocation when parsing GNU sparse map in archive/tar

[unknown] GO-2025-4015 (CVE-2025-61724) — stdlib@1.22.12

Excessive CPU consumption in Reader.ReadResponse in net/textproto

[unknown] GO-2025-4015 (CVE-2025-61724) — stdlib@1.23.6

Excessive CPU consumption in Reader.ReadResponse in net/textproto

[unknown] GO-2025-4096 (CVE-2025-31133) — runc@v1.1.12

Container escape via "masked path" abuse due to mount race conditions in github.com/opencontainers/runc

[unknown] GO-2025-4097 (CVE-2025-52565) — runc@v1.1.12

Container escape with malicious config due to /dev/console mount and related races in github.com/opencontainers/runc

[unknown] GO-2025-4098 (CVE-2025-52881) — runc@v1.1.12

Container escape and DDoS due to arbitrary write gadgets and procfs write redirects in github.com/opencontainers/runc

[unknown] GO-2025-4098 (CVE-2025-52881) — selinux@v1.11.0

Container escape and DDoS due to arbitrary write gadgets and procfs write redirects in github.com/opencontainers/runc

[unknown] GO-2025-4100 (CVE-2024-25621) — containerd@v1.7.11

containerd affected by a local privilege escalation via wide permissions on CRI directory in github.com/containerd/containerd

[unknown] GO-2025-4102 (CVE-2025-64437) — kubevirt@UNKNOWN

KubeVirt Isolation Detection Flaw Allows Arbitrary File Permission Changes in kubevirt.io/kubevirt

[unknown] GO-2025-4103 (CVE-2025-64432) — kubevirt@UNKNOWN

KubeVirt Affected by an Authentication Bypass in Kubernetes Aggregation Layer in kubevirt.io/kubevirt

[unknown] GO-2025-4105 (CVE-2025-64435) — kubevirt@UNKNOWN

KubeVirt VMI Denial-of-Service (DoS) Using Pod Impersonation in kubevirt.io/kubevirt

[unknown] GO-2025-4107 (CVE-2025-64434) — kubevirt@UNKNOWN

KubeVirt Improper TLS Certificate Management Handling Allows API Identity Spoofing in kubevirt.io/kubevirt

[unknown] GO-2025-4108 (CVE-2025-64329) — containerd@v1.7.11

containerd CRI server: Host memory exhaustion through Attach goroutine leak in github.com/containerd/containerd

[unknown] GO-2025-4109 (CVE-2025-64433) — kubevirt@UNKNOWN

KubeVirt Arbitrary Container File Read in kubevirt.io/kubevirt

[unknown] GO-2025-4110 (CVE-2025-64324) — kubevirt@UNKNOWN

KubeVirt Vulnerable to Arbitrary Host File Read and Write in kubevirt.io/kubevirt

[unknown] GO-2025-4116 (CVE-2025-47913) — crypto@v0.32.0

Potential denial of service in golang.org/x/crypto/ssh/agent

[unknown] GO-2025-4116 (CVE-2025-47913) — crypto@v0.33.0

Potential denial of service in golang.org/x/crypto/ssh/agent

[unknown] GO-2025-4116 (CVE-2025-47913) — crypto@v0.39.0

Potential denial of service in golang.org/x/crypto/ssh/agent

[unknown] GO-2025-4134 (CVE-2025-58181) — crypto@v0.32.0

Unbounded memory consumption in golang.org/x/crypto/ssh

[unknown] GO-2025-4134 (CVE-2025-58181) — crypto@v0.33.0

Unbounded memory consumption in golang.org/x/crypto/ssh

[unknown] GO-2025-4134 (CVE-2025-58181) — crypto@v0.39.0

Unbounded memory consumption in golang.org/x/crypto/ssh

[unknown] GO-2025-4135 (CVE-2025-47914) — crypto@v0.32.0

Malformed constraint may cause denial of service in golang.org/x/crypto/ssh/agent

[unknown] GO-2025-4135 (CVE-2025-47914) — crypto@v0.33.0

Malformed constraint may cause denial of service in golang.org/x/crypto/ssh/agent

[unknown] GO-2025-4135 (CVE-2025-47914) — crypto@v0.39.0

Malformed constraint may cause denial of service in golang.org/x/crypto/ssh/agent

[unknown] GO-2025-4155 (CVE-2025-61729) — stdlib@1.22.12

Excessive resource consumption when printing error string for host certificate validation in crypto/x509

[unknown] GO-2025-4155 (CVE-2025-61729) — stdlib@1.23.6

Excessive resource consumption when printing error string for host certificate validation in crypto/x509

[unknown] GO-2025-4175 (CVE-2025-61727) — stdlib@1.22.12

Improper application of excluded DNS name constraints when verifying wildcard names in crypto/x509

[unknown] GO-2025-4175 (CVE-2025-61727) — stdlib@1.23.6

Improper application of excluded DNS name constraints when verifying wildcard names in crypto/x509

[unknown] GO-2025-4192 (CVE-2025-66564) — timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing in github.com/sigstore/timestamp-authority

[unknown] GO-2025-4193 (CVE-2025-66506) — fulcio@v1.4.3

Fulcio allocates excessive memory during token parsing in github.com/sigstore/fulcio

[unknown] GO-2025-4193 (CVE-2025-66506) — fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing in github.com/sigstore/fulcio

[unknown] GO-2026-4309 (CVE-2026-22703) — v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions in github.com/sigstore/cosign

[unknown] GO-2026-4311 (CVE-2026-22772) — fulcio@v1.4.3

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass in github.com/sigstore/fulcio

[unknown] GO-2026-4311 (CVE-2026-22772) — fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass in github.com/sigstore/fulcio

[unknown] GO-2026-4316 (CVE-2025-69725) — chi@v4.1.2+incompatible

Open redirect vulnerability in the RedirectSlashes middleware in github.com/go-chi/chi

[unknown] GO-2026-4337 (CVE-2025-68121) — stdlib@1.22.12

Unexpected session resumption in crypto/tls

[unknown] GO-2026-4337 (CVE-2025-68121) — stdlib@1.23.6

Unexpected session resumption in crypto/tls

[unknown] GO-2026-4337 (CVE-2025-68121) — stdlib@1.25.5

Unexpected session resumption in crypto/tls

[unknown] GO-2026-4340 (CVE-2025-61730) — stdlib@1.22.12

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] GO-2026-4340 (CVE-2025-61730) — stdlib@1.23.6

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] GO-2026-4340 (CVE-2025-61730) — stdlib@1.25.5

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] GO-2026-4341 (CVE-2025-61726) — stdlib@1.22.12

Memory exhaustion in query parameter parsing in net/url

[unknown] GO-2026-4341 (CVE-2025-61726) — stdlib@1.23.6

Memory exhaustion in query parameter parsing in net/url

[unknown] GO-2026-4341 (CVE-2025-61726) — stdlib@1.25.5

Memory exhaustion in query parameter parsing in net/url

[unknown] GO-2026-4342 (CVE-2025-61728) — stdlib@1.22.12

Excessive CPU consumption when building archive index in archive/zip

[unknown] GO-2026-4342 (CVE-2025-61728) — stdlib@1.23.6

Excessive CPU consumption when building archive index in archive/zip

[unknown] GO-2026-4342 (CVE-2025-61728) — stdlib@1.25.5

Excessive CPU consumption when building archive index in archive/zip

[unknown] GO-2026-4348 (CVE-2026-23991) — v2@v2.0.2

Client DoS via malformed server response in github.com/theupdateframework/go-tuf

[unknown] GO-2026-4349 (CVE-2026-23992) — v2@v2.0.2

Improper validattion of configured threshold for delegations in github.com/theupdateframework/go-tuf

[unknown] GO-2026-4354 (CVE-2026-23831) — rekor@v1.2.2

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message in github.com/sigstore/rekor

[unknown] GO-2026-4354 (CVE-2026-23831) — rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message in github.com/sigstore/rekor

[unknown] GO-2026-4355 (CVE-2026-24117) — rekor@v1.2.2

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL in github.com/sigstore/rekor

[unknown] GO-2026-4355 (CVE-2026-24117) — rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL in github.com/sigstore/rekor

[unknown] GO-2026-4358 (CVE-2026-24137) — sigstore@v1.8.15

Sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal in github.com/sigstore/sigstore

[unknown] GO-2026-4358 (CVE-2026-24137) — sigstore@v1.8.2

Sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal in github.com/sigstore/sigstore

[unknown] GO-2026-4377 (CVE-2026-24686) — v2@v2.0.2

Path traversal in TAP 4 multirepo client allows arbitrary file write via repo names in github.com/theupdateframework/go-tuf

[unknown] GO-2026-4384 (CVE-2025-14525) — kubevirt@UNKNOWN

KubeVirt Guest Agent DoS via Excessive Network Interface Reports in kubevirt.io/kubevirt

[unknown] GO-2026-4394 (CVE-2026-24051) — sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking in go.opentelemetry.io/otel/sdk

[unknown] GO-2026-4403 (CVE-2025-22873) — stdlib@1.22.12

Improper access to parent directory of root in os

[unknown] GO-2026-4403 (CVE-2025-22873) — stdlib@1.23.6

Improper access to parent directory of root in os

[unknown] GO-2026-4440 (CVE-2025-47911) — net@v0.33.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] GO-2026-4440 (CVE-2025-47911) — net@v0.34.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] GO-2026-4440 (CVE-2025-47911) — net@v0.35.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] GO-2026-4440 (CVE-2025-47911) — net@v0.41.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] GO-2026-4441 (CVE-2025-58190) — net@v0.33.0

Infinite parsing loop in golang.org/x/net

[unknown] GO-2026-4441 (CVE-2025-58190) — net@v0.34.0

Infinite parsing loop in golang.org/x/net

[unknown] GO-2026-4441 (CVE-2025-58190) — net@v0.35.0

Infinite parsing loop in golang.org/x/net

[unknown] GO-2026-4441 (CVE-2025-58190) — net@v0.41.0

Infinite parsing loop in golang.org/x/net

[unknown] GO-2026-4473 (CVE-2026-25934) — v5@v5.11.0

Improper verification of data integrity values for .idx and .pack files in github.com/go-git/go-git

[unknown] GO-2026-4473 (CVE-2026-25934) — v5@v5.13.2

Improper verification of data integrity values for .idx and .pack files in github.com/go-git/go-git

[unknown] GO-2026-4529 (CVE-2026-24122) — v2@v2.4.3

Cosign considered signatures valid with expired intermediate certificates when transparency log verification is skipped in github.com/sigstore/cosign

[unknown] GO-2026-4550 (CVE-2026-1229) — circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult in github.com/cloudflare/circl

[unknown] GO-2026-4550 (CVE-2026-1229) — circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult in github.com/cloudflare/circl

[unknown] GO-2026-4569 (CVE-2026-27896) — go-sdk@v1.1.0

MCP Go SDK Vulnerable to Improper Handling of Case Sensitivity in github.com/modelcontextprotocol/go-sdk

[unknown] GO-2026-4601 (CVE-2026-25679) — stdlib@1.22.12

Incorrect parsing of IPv6 host literals in net/url

[unknown] GO-2026-4601 (CVE-2026-25679) — stdlib@1.23.6

Incorrect parsing of IPv6 host literals in net/url

[unknown] GO-2026-4601 (CVE-2026-25679) — stdlib@1.25.5

Incorrect parsing of IPv6 host literals in net/url

[unknown] GO-2026-4602 (CVE-2026-27139) — stdlib@1.22.12

FileInfo can escape from a Root in os

[unknown] GO-2026-4602 (CVE-2026-27139) — stdlib@1.23.6

FileInfo can escape from a Root in os

[unknown] GO-2026-4602 (CVE-2026-27139) — stdlib@1.25.5

FileInfo can escape from a Root in os

[unknown] GO-2026-4603 (CVE-2026-27142) — stdlib@1.22.12

URLs in meta content attribute actions are not escaped in html/template

[unknown] GO-2026-4603 (CVE-2026-27142) — stdlib@1.23.6

URLs in meta content attribute actions are not escaped in html/template

[unknown] GO-2026-4603 (CVE-2026-27142) — stdlib@1.25.5

URLs in meta content attribute actions are not escaped in html/template

[unknown] GO-2026-4610 (CVE-2025-15558) — cli@v27.4.1+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows in github.com/docker/cli

[unknown] GO-2026-4610 (CVE-2025-15558) — cli@v28.0.0+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows in github.com/docker/cli

[unknown] GO-2026-4730 (CVE-2026-33022) — pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun in github.com/tektoncd/pipeline

[unknown] GO-2026-4730 (CVE-2026-33022) — pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun in github.com/tektoncd/pipeline

[unknown] GO-2026-4762 (CVE-2026-33186) — grpc@v1.67.1

Authorization bypass in gRPC-Go via missing leading slash in :path in google.golang.org/grpc

[unknown] GO-2026-4762 (CVE-2026-33186) — grpc@v1.69.4

Authorization bypass in gRPC-Go via missing leading slash in :path in google.golang.org/grpc

[unknown] GO-2026-4762 (CVE-2026-33186) — grpc@v1.70.0

Authorization bypass in gRPC-Go via missing leading slash in :path in google.golang.org/grpc

[unknown] GO-2026-4770 — go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

[unknown] GO-2026-4773 (CVE-2026-33252) — go-sdk@v1.1.0

Cross-Site Tool Execution for HTTP Servers without Authorizatrion in github.com/modelcontextprotocol/go-sdk

[unknown] GO-2026-4858 (CVE-2026-33747) — buildkit@v0.12.5

BuildKit's Malicious frontend can cause file escape outside of storage root in github.com/moby/buildkit

[unknown] GO-2026-4858 (CVE-2026-33747) — buildkit@v0.16.0

BuildKit's Malicious frontend can cause file escape outside of storage root in github.com/moby/buildkit

[unknown] GO-2026-4859 (CVE-2026-33748) — buildkit@v0.12.5

BuildKit Git URL subdir component can cause access to restricted files in github.com/moby/buildkit

[unknown] GO-2026-4859 (CVE-2026-33748) — buildkit@v0.16.0

BuildKit Git URL subdir component can cause access to restricted files in github.com/moby/buildkit

[unknown] GO-2026-4864 (CVE-2026-32282) — stdlib@1.22.12

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] GO-2026-4864 (CVE-2026-32282) — stdlib@1.23.6

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] GO-2026-4864 (CVE-2026-32282) — stdlib@1.25.5

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] GO-2026-4865 (CVE-2026-32289) — stdlib@1.22.12

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] GO-2026-4865 (CVE-2026-32289) — stdlib@1.23.6

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] GO-2026-4865 (CVE-2026-32289) — stdlib@1.25.5

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] GO-2026-4869 (CVE-2026-32288) — stdlib@1.22.12

Unbounded allocation for old GNU sparse in archive/tar

[unknown] GO-2026-4869 (CVE-2026-32288) — stdlib@1.23.6

Unbounded allocation for old GNU sparse in archive/tar

[unknown] GO-2026-4869 (CVE-2026-32288) — stdlib@1.25.5

Unbounded allocation for old GNU sparse in archive/tar

[unknown] GO-2026-4870 (CVE-2026-32283) — stdlib@1.22.12

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] GO-2026-4870 (CVE-2026-32283) — stdlib@1.23.6

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] GO-2026-4870 (CVE-2026-32283) — stdlib@1.25.5

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] GO-2026-4883 (CVE-2026-33997) — docker@v25.0.6+incompatible

Moby has an Off-by-one error in its plugin privilege validation in github.com/docker/docker

[unknown] GO-2026-4883 (CVE-2026-33997) — docker@v27.4.1+incompatible

Moby has an Off-by-one error in its plugin privilege validation in github.com/docker/docker

[unknown] GO-2026-4883 (CVE-2026-33997) — docker@v28.0.0+incompatible

Moby has an Off-by-one error in its plugin privilege validation in github.com/docker/docker

[unknown] GO-2026-4887 (CVE-2026-34040) — docker@v25.0.6+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[unknown] GO-2026-4887 (CVE-2026-34040) — docker@v27.4.1+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[unknown] GO-2026-4887 (CVE-2026-34040) — docker@v28.0.0+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[unknown] GO-2026-4909 (CVE-2026-33762) — v5@v5.11.0

Missing validation decoding Index v4 files leads to panic in github.com/go-git/go-git

[unknown] GO-2026-4909 (CVE-2026-33762) — v5@v5.13.2

Missing validation decoding Index v4 files leads to panic in github.com/go-git/go-git

[unknown] GO-2026-4910 (CVE-2026-34165) — v5@v5.11.0

Maliciously crafted idx file can cause asymmetric memory consumption in github.com/go-git/go-git

[unknown] GO-2026-4910 (CVE-2026-34165) — v5@v5.13.2

Maliciously crafted idx file can cause asymmetric memory consumption in github.com/go-git/go-git

[unknown] GO-2026-4918 (CVE-2026-33814) — net@v0.33.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — net@v0.34.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — net@v0.35.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — net@v0.41.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — net@v0.52.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — stdlib@1.22.12

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — stdlib@1.23.6

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — stdlib@1.25.5

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — stdlib@1.25.9

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4918 (CVE-2026-33814) — stdlib@1.26.2

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] GO-2026-4942 (CVE-2026-35172) — v3@v3.0.0-20230519140516-983358f8e250

Stale blob descriptor cache invalidation in github.com/distribution/distribution

[unknown] GO-2026-4945 (CVE-2026-34986) — v3@v3.0.3

Go JOSE Panics in JWE decryption in github.com/go-jose/go-jose

[unknown] GO-2026-4945 (CVE-2026-34986) — v4@v4.0.5

Go JOSE Panics in JWE decryption in github.com/go-jose/go-jose

[unknown] GO-2026-4946 (CVE-2026-32281) — stdlib@1.22.12

Inefficient policy validation in crypto/x509

[unknown] GO-2026-4946 (CVE-2026-32281) — stdlib@1.23.6

Inefficient policy validation in crypto/x509

[unknown] GO-2026-4946 (CVE-2026-32281) — stdlib@1.25.5

Inefficient policy validation in crypto/x509

[unknown] GO-2026-4947 (CVE-2026-32280) — stdlib@1.22.12

Unexpected work during chain building in crypto/x509

[unknown] GO-2026-4947 (CVE-2026-32280) — stdlib@1.23.6

Unexpected work during chain building in crypto/x509

[unknown] GO-2026-4947 (CVE-2026-32280) — stdlib@1.25.5

Unexpected work during chain building in crypto/x509

[unknown] GO-2026-4958 (CVE-2026-35469) — spdystream@v0.2.0

Uncontrolled resource consumption when parsing SPDY frames in github.com/moby/spdystream

[unknown] GO-2026-4958 (CVE-2026-35469) — spdystream@v0.4.0

Uncontrolled resource consumption when parsing SPDY frames in github.com/moby/spdystream

[unknown] GO-2026-4958 (CVE-2026-35469) — spdystream@v0.5.0

Uncontrolled resource consumption when parsing SPDY frames in github.com/moby/spdystream

[unknown] GO-2026-4970 (CVE-2026-39822) — stdlib@1.22.12

Root escape via symlink plus trailing slash in os

[unknown] GO-2026-4970 (CVE-2026-39822) — stdlib@1.23.6

Root escape via symlink plus trailing slash in os

[unknown] GO-2026-4970 (CVE-2026-39822) — stdlib@1.25.5

Root escape via symlink plus trailing slash in os

[unknown] GO-2026-4970 (CVE-2026-39822) — stdlib@1.25.9

Root escape via symlink plus trailing slash in os

[unknown] GO-2026-4970 (CVE-2026-39822) — stdlib@1.26.2

Root escape via symlink plus trailing slash in os

[unknown] GO-2026-4971 (CVE-2026-39836) — stdlib@1.22.12

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] GO-2026-4971 (CVE-2026-39836) — stdlib@1.23.6

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] GO-2026-4971 (CVE-2026-39836) — stdlib@1.25.5

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] GO-2026-4971 (CVE-2026-39836) — stdlib@1.25.9

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] GO-2026-4971 (CVE-2026-39836) — stdlib@1.26.2

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] GO-2026-4976 (CVE-2026-39825) — stdlib@1.22.12

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] GO-2026-4976 (CVE-2026-39825) — stdlib@1.23.6

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] GO-2026-4976 (CVE-2026-39825) — stdlib@1.25.5

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] GO-2026-4976 (CVE-2026-39825) — stdlib@1.25.9

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] GO-2026-4976 (CVE-2026-39825) — stdlib@1.26.2

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] GO-2026-4977 (CVE-2026-42499) — stdlib@1.22.12

Quadratic string concatenation in consumePhrase in net/mail

[unknown] GO-2026-4977 (CVE-2026-42499) — stdlib@1.23.6

Quadratic string concatenation in consumePhrase in net/mail

[unknown] GO-2026-4977 (CVE-2026-42499) — stdlib@1.25.5

Quadratic string concatenation in consumePhrase in net/mail

[unknown] GO-2026-4977 (CVE-2026-42499) — stdlib@1.25.9

Quadratic string concatenation in consumePhrase in net/mail

[unknown] GO-2026-4977 (CVE-2026-42499) — stdlib@1.26.2

Quadratic string concatenation in consumePhrase in net/mail

[unknown] GO-2026-4980 (CVE-2026-39826) — stdlib@1.22.12

Escaper bypass leads to XSS in html/template

[unknown] GO-2026-4980 (CVE-2026-39826) — stdlib@1.23.6

Escaper bypass leads to XSS in html/template

[unknown] GO-2026-4980 (CVE-2026-39826) — stdlib@1.25.5

Escaper bypass leads to XSS in html/template

[unknown] GO-2026-4980 (CVE-2026-39826) — stdlib@1.25.9

Escaper bypass leads to XSS in html/template

[unknown] GO-2026-4980 (CVE-2026-39826) — stdlib@1.26.2

Escaper bypass leads to XSS in html/template

[unknown] GO-2026-4981 (CVE-2026-33811) — stdlib@1.22.12

Crash when handling long CNAME response in net

[unknown] GO-2026-4981 (CVE-2026-33811) — stdlib@1.23.6

Crash when handling long CNAME response in net

[unknown] GO-2026-4981 (CVE-2026-33811) — stdlib@1.25.5

Crash when handling long CNAME response in net

[unknown] GO-2026-4981 (CVE-2026-33811) — stdlib@1.25.9

Crash when handling long CNAME response in net

[unknown] GO-2026-4981 (CVE-2026-33811) — stdlib@1.26.2

Crash when handling long CNAME response in net

[unknown] GO-2026-4982 (CVE-2026-39823) — stdlib@1.22.12

Bypass of meta content URL escaping causes XSS in html/template

[unknown] GO-2026-4982 (CVE-2026-39823) — stdlib@1.23.6

Bypass of meta content URL escaping causes XSS in html/template

[unknown] GO-2026-4982 (CVE-2026-39823) — stdlib@1.25.5

Bypass of meta content URL escaping causes XSS in html/template

[unknown] GO-2026-4982 (CVE-2026-39823) — stdlib@1.25.9

Bypass of meta content URL escaping causes XSS in html/template

[unknown] GO-2026-4982 (CVE-2026-39823) — stdlib@1.26.2

Bypass of meta content URL escaping causes XSS in html/template

[unknown] GO-2026-4986 (CVE-2026-39820) — stdlib@1.22.12

Quadratic string concatentation in consumeComment in net/mail

[unknown] GO-2026-4986 (CVE-2026-39820) — stdlib@1.23.6

Quadratic string concatentation in consumeComment in net/mail

[unknown] GO-2026-4986 (CVE-2026-39820) — stdlib@1.25.5

Quadratic string concatentation in consumeComment in net/mail

[unknown] GO-2026-4986 (CVE-2026-39820) — stdlib@1.25.9

Quadratic string concatentation in consumeComment in net/mail

[unknown] GO-2026-4986 (CVE-2026-39820) — stdlib@1.26.2

Quadratic string concatentation in consumeComment in net/mail

[unknown] GO-2026-5005 (CVE-2026-39833) — crypto@v0.32.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5005 (CVE-2026-39833) — crypto@v0.33.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5005 (CVE-2026-39833) — crypto@v0.39.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5005 (CVE-2026-39833) — crypto@v0.49.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5006 (CVE-2026-39832) — crypto@v0.32.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5006 (CVE-2026-39832) — crypto@v0.33.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5006 (CVE-2026-39832) — crypto@v0.39.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5006 (CVE-2026-39832) — crypto@v0.49.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5013 (CVE-2026-46597) — crypto@v0.32.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] GO-2026-5013 (CVE-2026-46597) — crypto@v0.33.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] GO-2026-5013 (CVE-2026-46597) — crypto@v0.39.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] GO-2026-5013 (CVE-2026-46597) — crypto@v0.49.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] GO-2026-5014 (CVE-2026-39828) — crypto@v0.32.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] GO-2026-5014 (CVE-2026-39828) — crypto@v0.33.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] GO-2026-5014 (CVE-2026-39828) — crypto@v0.39.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] GO-2026-5014 (CVE-2026-39828) — crypto@v0.49.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] GO-2026-5015 (CVE-2026-39835) — crypto@v0.32.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] GO-2026-5015 (CVE-2026-39835) — crypto@v0.33.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] GO-2026-5015 (CVE-2026-39835) — crypto@v0.39.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] GO-2026-5015 (CVE-2026-39835) — crypto@v0.49.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] GO-2026-5016 (CVE-2026-39827) — crypto@v0.32.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5016 (CVE-2026-39827) — crypto@v0.33.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5016 (CVE-2026-39827) — crypto@v0.39.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5016 (CVE-2026-39827) — crypto@v0.49.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5017 (CVE-2026-39830) — crypto@v0.32.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] GO-2026-5017 (CVE-2026-39830) — crypto@v0.33.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] GO-2026-5017 (CVE-2026-39830) — crypto@v0.39.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] GO-2026-5017 (CVE-2026-39830) — crypto@v0.49.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] GO-2026-5018 (CVE-2026-39829) — crypto@v0.32.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5018 (CVE-2026-39829) — crypto@v0.33.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5018 (CVE-2026-39829) — crypto@v0.39.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5018 (CVE-2026-39829) — crypto@v0.49.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] GO-2026-5019 (CVE-2026-39831) — crypto@v0.32.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] GO-2026-5019 (CVE-2026-39831) — crypto@v0.33.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] GO-2026-5019 (CVE-2026-39831) — crypto@v0.39.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] GO-2026-5019 (CVE-2026-39831) — crypto@v0.49.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] GO-2026-5020 (CVE-2026-39834) — crypto@v0.32.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] GO-2026-5020 (CVE-2026-39834) — crypto@v0.33.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] GO-2026-5020 (CVE-2026-39834) — crypto@v0.39.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] GO-2026-5020 (CVE-2026-39834) — crypto@v0.49.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] GO-2026-5021 (CVE-2026-42508) — crypto@v0.32.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] GO-2026-5021 (CVE-2026-42508) — crypto@v0.33.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] GO-2026-5021 (CVE-2026-42508) — crypto@v0.39.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] GO-2026-5021 (CVE-2026-42508) — crypto@v0.49.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] GO-2026-5023 (CVE-2026-46595) — crypto@v0.32.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] GO-2026-5023 (CVE-2026-46595) — crypto@v0.33.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] GO-2026-5023 (CVE-2026-46595) — crypto@v0.39.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] GO-2026-5023 (CVE-2026-46595) — crypto@v0.49.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] GO-2026-5024 (CVE-2026-39824) — sys@v0.29.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] GO-2026-5024 (CVE-2026-39824) — sys@v0.30.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] GO-2026-5024 (CVE-2026-39824) — sys@v0.33.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] GO-2026-5024 (CVE-2026-39824) — sys@v0.42.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] GO-2026-5025 (CVE-2026-42506) — net@v0.33.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5025 (CVE-2026-42506) — net@v0.34.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5025 (CVE-2026-42506) — net@v0.35.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5025 (CVE-2026-42506) — net@v0.41.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5025 (CVE-2026-42506) — net@v0.52.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5026 (CVE-2026-39821) — net@v0.33.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — net@v0.34.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — net@v0.35.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — net@v0.41.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — net@v0.52.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — stdlib@1.22.12

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — stdlib@1.23.6

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — stdlib@1.25.5

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — stdlib@1.25.9

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — stdlib@1.26.2

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5026 (CVE-2026-39821) — stdlib@1.26.5

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5027 (CVE-2026-42502) — net@v0.33.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5027 (CVE-2026-42502) — net@v0.34.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5027 (CVE-2026-42502) — net@v0.35.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5027 (CVE-2026-42502) — net@v0.41.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5027 (CVE-2026-42502) — net@v0.52.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] GO-2026-5028 (CVE-2026-25680) — net@v0.33.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] GO-2026-5028 (CVE-2026-25680) — net@v0.34.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] GO-2026-5028 (CVE-2026-25680) — net@v0.35.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] GO-2026-5028 (CVE-2026-25680) — net@v0.41.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] GO-2026-5028 (CVE-2026-25680) — net@v0.52.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] GO-2026-5029 (CVE-2026-25681) — net@v0.33.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] GO-2026-5029 (CVE-2026-25681) — net@v0.34.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] GO-2026-5029 (CVE-2026-25681) — net@v0.35.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] GO-2026-5029 (CVE-2026-25681) — net@v0.41.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] GO-2026-5029 (CVE-2026-25681) — net@v0.52.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] GO-2026-5030 (CVE-2026-27136) — net@v0.33.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] GO-2026-5030 (CVE-2026-27136) — net@v0.34.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] GO-2026-5030 (CVE-2026-27136) — net@v0.35.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] GO-2026-5030 (CVE-2026-27136) — net@v0.41.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] GO-2026-5030 (CVE-2026-27136) — net@v0.52.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] GO-2026-5033 (CVE-2026-46598) — crypto@v0.32.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5033 (CVE-2026-46598) — crypto@v0.33.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5033 (CVE-2026-46598) — crypto@v0.39.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5033 (CVE-2026-46598) — crypto@v0.49.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] GO-2026-5037 (CVE-2026-27145) — stdlib@1.22.12

Inefficient candidate hostname parsing in crypto/x509

[unknown] GO-2026-5037 (CVE-2026-27145) — stdlib@1.23.6

Inefficient candidate hostname parsing in crypto/x509

[unknown] GO-2026-5037 (CVE-2026-27145) — stdlib@1.25.5

Inefficient candidate hostname parsing in crypto/x509

[unknown] GO-2026-5037 (CVE-2026-27145) — stdlib@1.25.9

Inefficient candidate hostname parsing in crypto/x509

[unknown] GO-2026-5037 (CVE-2026-27145) — stdlib@1.26.2

Inefficient candidate hostname parsing in crypto/x509

[unknown] GO-2026-5038 (CVE-2026-42504) — stdlib@1.22.12

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] GO-2026-5038 (CVE-2026-42504) — stdlib@1.23.6

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] GO-2026-5038 (CVE-2026-42504) — stdlib@1.25.5

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] GO-2026-5038 (CVE-2026-42504) — stdlib@1.25.9

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] GO-2026-5038 (CVE-2026-42504) — stdlib@1.26.2

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] GO-2026-5039 (CVE-2026-42507) — stdlib@1.22.12

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] GO-2026-5039 (CVE-2026-42507) — stdlib@1.23.6

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] GO-2026-5039 (CVE-2026-42507) — stdlib@1.25.5

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] GO-2026-5039 (CVE-2026-42507) — stdlib@1.25.9

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] GO-2026-5039 (CVE-2026-42507) — stdlib@1.26.2

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] GO-2026-5064 (CVE-2026-53492) — containerd@v1.7.11

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[unknown] GO-2026-5064 (CVE-2026-53492) — containerd@v1.7.32

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[unknown] GO-2026-5074 (CVE-2026-45022) — v5@v5.11.0

Go-git: Improper parsing of specially crafted objects may lead to inconsistent interpretation in github.com/go-git/go-git

[unknown] GO-2026-5074 (CVE-2026-45022) — v5@v5.13.2

Go-git: Improper parsing of specially crafted objects may lead to inconsistent interpretation in github.com/go-git/go-git

[unknown] GO-2026-5094 (CVE-2026-33540) — v3@v3.0.0-20230519140516-983358f8e250

Distribution affected by pull-through cache credential exfiltration via www-authenticate bearer realm in github.com/distribution/distribution

[unknown] GO-2026-5105 (CVE-2026-41506) — v5@v5.11.0

Go-git: Credential leak via cross-host redirect in smart HTTP transport in github.com/go-git/go-git

[unknown] GO-2026-5105 (CVE-2026-41506) — v5@v5.13.2

Go-git: Credential leak via cross-host redirect in smart HTTP transport in github.com/go-git/go-git

[unknown] GO-2026-5158 (CVE-2026-41178) — otel@v1.43.0

Opentelemetry-go's baggage parsing no longer caps raw header length in go.opentelemetry.io/otel

[unknown] GO-2026-5185 (CVE-2026-41888) — v3@v3.0.0-20230519140516-983358f8e250

Distribution's tag deletion bypasses `storage.delete.enabled` configuration in github.com/distribution/distribution

[unknown] GO-2026-5327 (CVE-2026-2303) — mongo-driver@v1.14.0

Mongo-go-driver: Heap Out-of-Bounds Read in GSSAPI Error Handling in go.mongodb.org/mongo-driver

[unknown] GO-2026-5327 (CVE-2026-2303) — mongo-driver@v1.16.1

Mongo-go-driver: Heap Out-of-Bounds Read in GSSAPI Error Handling in go.mongodb.org/mongo-driver

[unknown] GO-2026-5336 (CVE-2026-45571) — v5@v5.11.0

Go-git: Crafted repositories may modify main and submodule .git directories in github.com/go-git/go-git

[unknown] GO-2026-5336 (CVE-2026-45571) — v5@v5.13.2

Go-git: Crafted repositories may modify main and submodule .git directories in github.com/go-git/go-git

[unknown] GO-2026-5338 (CVE-2026-50195) — containerd@v1.7.11

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[unknown] GO-2026-5338 (CVE-2026-50195) — containerd@v1.7.32

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[unknown] GO-2026-5426 (CVE-2026-39883) — sdk@v1.34.0

Opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking in go.opentelemetry.io/otel/sdk

[unknown] GO-2026-5435 (CVE-2026-35206) — v3@UNKNOWN

Helm Chart extraction output directory collapse via Chart.yaml name dot-segment in helm.sh/helm

[unknown] GO-2026-5450 (CVE-2026-6383) — kubevirt@UNKNOWN

KubeVirt's authorization mechanism improperly truncates subresource names in kubevirt.io/kubevirt

[unknown] GO-2026-5475 (CVE-2026-47262) — containerd@v1.7.11

containerd image-triggered runtime DoS via unbounded group parsing in github.com/containerd/containerd

[unknown] GO-2026-5475 (CVE-2026-47262) — containerd@v1.7.32

containerd image-triggered runtime DoS via unbounded group parsing in github.com/containerd/containerd

[unknown] GO-2026-5490 (CVE-2026-44740) — v5@v5.5.0

Go-billy: Symlink resolution lack of cycle detection leads to infinite loop in github.com/go-git/go-billy

[unknown] GO-2026-5490 (CVE-2026-44740) — v5@v5.6.2

Go-billy: Symlink resolution lack of cycle detection leads to infinite loop in github.com/go-git/go-billy

[unknown] GO-2026-5496 (CVE-2026-45570) — v5@v5.11.0

Improper single-quote escaping in go-git SSH transport in github.com/go-git/go-git

[unknown] GO-2026-5496 (CVE-2026-45570) — v5@v5.13.2

Improper single-quote escaping in go-git SSH transport in github.com/go-git/go-git

[unknown] GO-2026-5547 — in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior in github.com/in-toto/in-toto-golang

[unknown] GO-2026-5597 (CVE-2026-44973) — v5@v5.5.0

Go-billy has path traversal vulnerabilities in github.com/go-git/go-billy

[unknown] GO-2026-5597 (CVE-2026-44973) — v5@v5.6.2

Go-billy has path traversal vulnerabilities in github.com/go-git/go-billy

[unknown] GO-2026-5617 (CVE-2026-42306) — docker@v25.0.6+incompatible

Race condition in 'docker cp' in github.com/docker/docker allows bind mount redirection

[unknown] GO-2026-5617 (CVE-2026-42306) — docker@v27.4.1+incompatible

Race condition in 'docker cp' in github.com/docker/docker allows bind mount redirection

[unknown] GO-2026-5617 (CVE-2026-42306) — docker@v28.0.0+incompatible

Race condition in 'docker cp' in github.com/docker/docker allows bind mount redirection

[unknown] GO-2026-5622 (CVE-2026-53489) — containerd@v1.7.11

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[unknown] GO-2026-5622 (CVE-2026-53489) — containerd@v1.7.32

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[unknown] GO-2026-5630 (CVE-2026-25542) — pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching in github.com/tektoncd/pipeline

[unknown] GO-2026-5630 (CVE-2026-25542) — pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching in github.com/tektoncd/pipeline

[unknown] GO-2026-5668 (CVE-2026-41568) — docker@v25.0.6+incompatible

Race condition in 'docker cp' in github.com/docker/docker allows creation of arbitrary files

[unknown] GO-2026-5668 (CVE-2026-41568) — docker@v27.4.1+incompatible

Race condition in 'docker cp' in github.com/docker/docker allows creation of arbitrary files

[unknown] GO-2026-5668 (CVE-2026-41568) — docker@v28.0.0+incompatible

Race condition in 'docker cp' in github.com/docker/docker allows creation of arbitrary files

[unknown] GO-2026-5693 — v5@v5.11.0

Go-git: Malformed Git object data may cause panics or resource exhaustion in github.com/go-git/go-git

[unknown] GO-2026-5693 — v5@v5.13.2

Go-git: Malformed Git object data may cause panics or resource exhaustion in github.com/go-git/go-git

[unknown] GO-2026-5694 (CVE-2026-39395) — v2@v2.4.3

Cosign's verify-blob-attestation reports false positive when payload parsing fails in github.com/sigstore/cosign

[unknown] GO-2026-5746 (CVE-2026-41567) — docker@v25.0.6+incompatible

Docker: 'PUT /containers/{id}/archive' executes container binary on the host in github.com/docker/docker

[unknown] GO-2026-5746 (CVE-2026-41567) — docker@v27.4.1+incompatible

Docker: 'PUT /containers/{id}/archive' executes container binary on the host in github.com/docker/docker

[unknown] GO-2026-5746 (CVE-2026-41567) — docker@v28.0.0+incompatible

Docker: 'PUT /containers/{id}/archive' executes container binary on the host in github.com/docker/docker

[unknown] GO-2026-5758 (CVE-2026-53488) — containerd@v1.7.11

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull in github.com/containerd/containerd

[unknown] GO-2026-5758 (CVE-2026-53488) — containerd@v1.7.32

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull in github.com/containerd/containerd

[unknown] GO-2026-5761 (CVE-2026-41579) — runc@v1.1.12

Malicious image with /dev symlink can trigger limited host filesystem integrity violations in github.com/opencontainers/runc

[unknown] GO-2026-5763 (CVE-2026-39984) — timestamp-authority@v1.2.4

Sigstore Timestamp Authority has Improper Certificate Validation in verifier in github.com/sigstore/timestamp-authority

[unknown] GO-2026-5764 (CVE-2026-89090) — eventstream@v1.6.8

DoS due to Panic in AWS SDK for Go v2 SDK EventStream Decoder in github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream

[unknown] GO-2026-5764 (CVE-2026-89090) — s3@v1.76.0

DoS due to Panic in AWS SDK for Go v2 SDK EventStream Decoder in github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream

[unknown] GO-2026-5771 (CVE-2026-34742) — go-sdk@v1.1.0

DNS Rebinding Protection Disabled by Default in Model Context Protocol Go SDK for Servers Running on Localhost in github.com/modelcontextprotocol/go-sdk

[unknown] GO-2026-5775 (CVE-2026-72817) — v5@v5.1.0

Chi Middleware vulnerable to IP spoofing via X-Forwarded-For header in github.com/go-chi/chi

[unknown] GO-2026-5777 (CVE-2026-72816) — v5@v5.1.0

Chi's RealIP Middleware allows IP spoofing via unvalidated X-Forwarded-For header in github.com/go-chi/chi

[unknown] GO-2026-5778 (CVE-2026-48702) — rekor@v1.2.2

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic in github.com/sigstore/rekor

[unknown] GO-2026-5778 (CVE-2026-48702) — rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic in github.com/sigstore/rekor

[unknown] GO-2026-5841 — compress@v1.17.11

OOB read in github.com/klauspost/compress/s2

[unknown] GO-2026-5841 — compress@v1.17.7

OOB read in github.com/klauspost/compress/s2

[unknown] GO-2026-5841 — compress@v1.18.4

OOB read in github.com/klauspost/compress/s2

[unknown] GO-2026-5848 (CVE-2026-7374) — kubevirt@UNKNOWN

KubeVirt has a Link Following vulnerability in kubevirt.io/kubevirt

[unknown] GO-2026-5851 (CVE-2026-49835) — timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality in github.com/sigstore/timestamp-authority

[unknown] GO-2026-5853 (CVE-2026-49478) — fulcio@v1.4.3

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage in github.com/sigstore/fulcio

[unknown] GO-2026-5853 (CVE-2026-49478) — fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage in github.com/sigstore/fulcio

[unknown] GO-2026-5856 (CVE-2026-42505) — stdlib@1.22.12

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] GO-2026-5856 (CVE-2026-42505) — stdlib@1.23.6

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] GO-2026-5856 (CVE-2026-42505) — stdlib@1.25.5

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] GO-2026-5856 (CVE-2026-42505) — stdlib@1.25.9

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] GO-2026-5856 (CVE-2026-42505) — stdlib@1.26.2

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] GO-2026-5880 (CVE-2026-50163) — v2@v2.6.1

Hardlink path traversal during tar extraction in oras.land/oras-go

[unknown] GO-2026-5883 (CVE-2026-9804) — kubevirt@UNKNOWN

KubeVirt has a Link Following issue in kubevirt.io/kubevirt

[unknown] GO-2026-5932 — crypto@v0.32.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — crypto@v0.33.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — crypto@v0.39.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — crypto@v0.49.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — crypto@v0.53.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.33.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.34.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.35.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.41.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.52.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.55.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — net@v0.55.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — stdlib@1.26.2

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5942 (CVE-2026-46600) — stdlib@1.26.5

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] GO-2026-5952 (CVE-2026-49834) — sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log in github.com/sigstore/sigstore-go

[unknown] GO-2026-5970 (CVE-2026-56852) — text@v0.21.0

Infinite loop on invalid input in golang.org/x/text

[unknown] GO-2026-5970 (CVE-2026-56852) — text@v0.22.0

Infinite loop on invalid input in golang.org/x/text

[unknown] GO-2026-5970 (CVE-2026-56852) — text@v0.26.0

Infinite loop on invalid input in golang.org/x/text

[unknown] GO-2026-5970 (CVE-2026-56852) — text@v0.35.0

Infinite loop on invalid input in golang.org/x/text

[unknown] GO-2026-5970 (CVE-2026-56852) — text@v0.37.0

Infinite loop on invalid input in golang.org/x/text

[unknown] GO-2026-5970 (CVE-2026-56852) — text@v0.38.0

Infinite loop on invalid input in golang.org/x/text

[unknown] GO-2026-5972 (CVE-2026-33818) — stdlib@1.22.12

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-5972 (CVE-2026-33818) — stdlib@1.23.6

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-5972 (CVE-2026-33818) — stdlib@1.25.5

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-5972 (CVE-2026-33818) — stdlib@1.25.9

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-5972 (CVE-2026-33818) — stdlib@1.26.2

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-5972 (CVE-2026-33818) — stdlib@1.26.5

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-6061 — grpc@v1.67.1

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — grpc@v1.69.4

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — grpc@v1.70.0

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — grpc@v1.79.3

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — grpc@v1.80.0

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6088 (CVE-2026-56859) — stdlib@1.22.12

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6088 (CVE-2026-56859) — stdlib@1.23.6

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6088 (CVE-2026-56859) — stdlib@1.25.5

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6088 (CVE-2026-56859) — stdlib@1.25.9

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6088 (CVE-2026-56859) — stdlib@1.26.2

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6088 (CVE-2026-56859) — stdlib@1.26.5

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6089 (CVE-2026-56853) — stdlib@1.22.12

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6089 (CVE-2026-56853) — stdlib@1.23.6

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6089 (CVE-2026-56853) — stdlib@1.25.5

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6089 (CVE-2026-56853) — stdlib@1.25.9

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6089 (CVE-2026-56853) — stdlib@1.26.2

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6089 (CVE-2026-56853) — stdlib@1.26.5

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6090 (CVE-2026-56862) — stdlib@1.22.12

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6090 (CVE-2026-56862) — stdlib@1.23.6

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6090 (CVE-2026-56862) — stdlib@1.25.5

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6090 (CVE-2026-56862) — stdlib@1.25.9

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6090 (CVE-2026-56862) — stdlib@1.26.2

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6090 (CVE-2026-56862) — stdlib@1.26.5

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6091 (CVE-2026-56858) — stdlib@1.22.12

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6091 (CVE-2026-56858) — stdlib@1.23.6

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6091 (CVE-2026-56858) — stdlib@1.25.5

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6091 (CVE-2026-56858) — stdlib@1.25.9

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6091 (CVE-2026-56858) — stdlib@1.26.2

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6091 (CVE-2026-56858) — stdlib@1.26.5

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6094 — cel-go@v0.23.2

JSON private fields exposed via NativeTypes and ParseStructTag in github.com/google/cel-go

[unknown] GO-2026-6162 (CVE-2026-54787) — sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period in github.com/sigstore/sigstore-go

[unknown] GO-2026-6179 (CVE-2026-56865) — mod@v0.22.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] GO-2026-6179 (CVE-2026-56865) — mod@v0.25.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] GO-2026-6179 (CVE-2026-56865) — mod@v0.33.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] GO-2026-6180 (CVE-2026-56864) — mod@v0.22.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] GO-2026-6180 (CVE-2026-56864) — mod@v0.25.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] GO-2026-6180 (CVE-2026-56864) — mod@v0.33.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] GO-2026-6213 (CVE-2026-71556) — v5@v5.11.0

Worktree operations may follow symlinks in github.com/go-git/go-git

[unknown] GO-2026-6213 (CVE-2026-71556) — v5@v5.13.2

Worktree operations may follow symlinks in github.com/go-git/go-git

[unknown] GO-2026-6214 (CVE-2026-71557) — v5@v5.11.0

Path traversal via crafted reference names in github.com/go-git/go-git

[unknown] GO-2026-6214 (CVE-2026-71557) — v5@v5.13.2

Path traversal via crafted reference names in github.com/go-git/go-git

[unknown] GO-2026-6218 (CVE-2026-56860) — stdlib@1.22.12

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6218 (CVE-2026-56860) — stdlib@1.23.6

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6218 (CVE-2026-56860) — stdlib@1.25.5

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6218 (CVE-2026-56860) — stdlib@1.25.9

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6218 (CVE-2026-56860) — stdlib@1.26.2

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6218 (CVE-2026-56860) — stdlib@1.26.5

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6225 — docker-credential-acr-env@v0.0.0-20230304212654-82a0ddb27589

Credential leakage to untrusted hosts in github.com/chrismellard/docker-credential-acr-env

[unknown] GO-2026-6255 (CVE-2026-61711) — buildkit@v0.12.5

BuildKit: Custom frontend could bypass Seccomp/AppArmor in github.com/moby/buildkit

[unknown] GO-2026-6255 (CVE-2026-61711) — buildkit@v0.16.0

BuildKit: Custom frontend could bypass Seccomp/AppArmor in github.com/moby/buildkit

[unknown] GO-2026-6256 (CVE-2026-61712) — buildkit@v0.12.5

BuildKit has a possible runtime DoS via unbounded group parsing in github.com/moby/buildkit

[unknown] GO-2026-6256 (CVE-2026-61712) — buildkit@v0.16.0

BuildKit has a possible runtime DoS via unbounded group parsing in github.com/moby/buildkit

[unknown] GO-2026-6263 (CVE-2026-54168) — pipelines-as-code@v0.31.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution in github.com/openshift-pipelines/pipelines-as-code

[unknown] GO-2026-6263 (CVE-2026-54168) — pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution in github.com/openshift-pipelines/pipelines-as-code

[unknown] GO-2026-6266 (CVE-2026-54167) — pipelines-as-code@v0.31.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header in github.com/openshift-pipelines/pipelines-as-code

[unknown] GO-2026-6266 (CVE-2026-54167) — pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header in github.com/openshift-pipelines/pipelines-as-code

[unknown] GO-2026-6278 — websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key in github.com/gorilla/websocket

[unknown] GO-2026-6278 — websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key in github.com/gorilla/websocket

[unknown] GO-2026-6278 — websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key in github.com/gorilla/websocket

[unknown] GO-2026-6303 (CVE-2026-56854) — crypto@v0.32.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] GO-2026-6303 (CVE-2026-56854) — crypto@v0.33.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] GO-2026-6303 (CVE-2026-56854) — crypto@v0.39.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] GO-2026-6303 (CVE-2026-56854) — crypto@v0.49.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] GO-2026-6303 (CVE-2026-56854) — crypto@v0.53.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] GO-2026-6348 (CVE-2026-84304) — grpc@v1.67.1

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] GO-2026-6348 (CVE-2026-84304) — grpc@v1.69.4

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] GO-2026-6348 (CVE-2026-84304) — grpc@v1.70.0

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] GO-2026-6348 (CVE-2026-84304) — grpc@v1.79.3

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] GO-2026-6348 (CVE-2026-84304) — grpc@v1.80.0

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] GO-2026-6354 (CVE-2026-78662) — crypto@v0.32.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6354 (CVE-2026-78662) — crypto@v0.33.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6354 (CVE-2026-78662) — crypto@v0.39.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6354 (CVE-2026-78662) — crypto@v0.49.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6354 (CVE-2026-78662) — crypto@v0.53.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6355 (CVE-2026-56855) — crypto@v0.32.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6355 (CVE-2026-56855) — crypto@v0.33.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6355 (CVE-2026-56855) — crypto@v0.39.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6355 (CVE-2026-56855) — crypto@v0.49.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6355 (CVE-2026-56855) — crypto@v0.53.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6441 (CVE-2026-84303) — grpc@v1.67.1

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] GO-2026-6441 (CVE-2026-84303) — grpc@v1.69.4

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] GO-2026-6441 (CVE-2026-84303) — grpc@v1.70.0

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] GO-2026-6441 (CVE-2026-84303) — grpc@v1.79.3

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] GO-2026-6441 (CVE-2026-84303) — grpc@v1.80.0

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] GO-2026-6443 (CVE-2026-84445) — grpc@v1.67.1

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] GO-2026-6443 (CVE-2026-84445) — grpc@v1.69.4

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] GO-2026-6443 (CVE-2026-84445) — grpc@v1.70.0

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] GO-2026-6443 (CVE-2026-84445) — grpc@v1.79.3

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] GO-2026-6443 (CVE-2026-84445) — grpc@v1.80.0

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] GO-2026-6444 (CVE-2026-53495) — containerd@v1.7.11

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service in github.com/containerd/containerd

[unknown] GO-2026-6444 (CVE-2026-53495) — containerd@v1.7.32

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service in github.com/containerd/containerd

Findings from bomber

[critical] CVE-2020-14316 — pkg:golang/kubevirt.io/kubevirt

Privilege Escalation in kubevirt

[critical] CVE-2025-21613 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git has an Argument Injection via the URL field

[critical] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go has an authorization bypass via missing leading slash in :path

[critical] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go has an authorization bypass via missing leading slash in :path

[critical] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go has an authorization bypass via missing leading slash in :path

[critical] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[critical] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[critical] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[critical] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses

[critical] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[critical] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[critical] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[critical] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed

[critical] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[critical] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[critical] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[critical] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

[critical] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto doesn't enforce invoking key constraints

[critical] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't enforce invoking key constraints

[critical] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto doesn't enforce invoking key constraints

[critical] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto doesn't enforce invoking key constraints

[critical] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[critical] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[critical] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[critical] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

[critical] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[critical] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[critical] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[critical] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

[critical] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[critical] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[critical] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[critical] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

[critical] CVE-2026-7374 — pkg:golang/kubevirt.io/kubevirt

KubeVirt has a Link Following vulnerability

[high] CVE-2020-11013 — pkg:golang/helm.sh/helm/v3

Lookup function information discolosure in helm

[high] CVE-2020-7919 — pkg:golang/helm.sh/helm/v3

Helm uses crypto package vulnerable to panic from malformed X.509 certificate

[high] CVE-2022-1798 — pkg:golang/kubevirt.io/kubevirt

KubeVirt vulnerable to arbitrary file read on host

[high] CVE-2023-26484 — pkg:golang/kubevirt.io/kubevirt

On a compromised node, the virt-handler service account can be used to modify all node specs

[high] CVE-2024-25621 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd affected by a local privilege escalation via wide permissions on CRI directory

[high] CVE-2024-26147 — pkg:golang/helm.sh/helm/v3

Helm's Missing YAML Content Leads To Panic

[high] CVE-2025-15558 — pkg:golang/github.com/docker/cli@v27.4.1%2Bincompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

[high] CVE-2025-15558 — pkg:golang/github.com/docker/cli@v28.0.0%2Bincompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows

[high] CVE-2025-21614 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git clients vulnerable to DoS via maliciously crafted Git server replies

[high] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.12.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[high] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.18.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[high] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.23.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[high] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.26.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

[high] CVE-2025-22869 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

[high] CVE-2025-22869 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

[high] CVE-2025-30204 — pkg:golang/github.com/golang-jwt/jwt/v4@v4.5.1

jwt-go allows excessive memory allocation during header parsing

[high] CVE-2025-30204 — pkg:golang/github.com/golang-jwt/jwt/v5@v5.2.1

jwt-go allows excessive memory allocation during header parsing

[high] CVE-2025-31133 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc container escape via "masked path" abuse due to mount race conditions

[high] CVE-2025-52565 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc container escape with malicious config due to /dev/console mount and related races

[high] CVE-2025-52881 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

[high] CVE-2025-52881 — pkg:golang/github.com/opencontainers/selinux@v1.11.0

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

[high] CVE-2025-53547 — pkg:golang/helm.sh/helm/v3

Helm vulnerable to Code Injection through malicious chart.yaml content

[high] CVE-2025-64324 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Vulnerable to Arbitrary Host File Read and Write

[high] CVE-2025-66506 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio allocates excessive memory during token parsing

[high] CVE-2025-66506 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing

[high] CVE-2025-66564 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing

[high] CVE-2026-24051 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking

[high] CVE-2026-27896 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

MCP Go SDK Vulnerable to Improper Handling of Case Sensitivity

[high] CVE-2026-33252 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Cross-Site Tool Execution for HTTP Servers without Authorizatrion in github.com/modelcontextprotocol/go-sdk

[high] CVE-2026-33540 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution affected by pull-through cache credential exfiltration via www-authenticate bearer realm

[high] CVE-2026-33747 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit's Malicious frontend can cause file escape outside of storage root

[high] CVE-2026-33747 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit's Malicious frontend can cause file escape outside of storage root

[high] CVE-2026-33748 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit Git URL subdir component can cause access to restricted files

[high] CVE-2026-33748 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit Git URL subdir component can cause access to restricted files

[high] CVE-2026-34742 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

DNS Rebinding Protection Disabled by Default in Model Context Protocol Go SDK for Servers Running on Localhost

[high] CVE-2026-34986 — pkg:golang/github.com/go-jose/go-jose/v3@v3.0.3

Go JOSE Panics in JWE decryption

[high] CVE-2026-34986 — pkg:golang/github.com/go-jose/go-jose/v4@v4.0.5

Go JOSE Panics in JWE decryption

[high] CVE-2026-35172 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution: stale blob access resurrection via repo-scoped redis descriptor cache invalidation

[high] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.2.0

SpdyStream: DOS on CRI

[high] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.4.0

SpdyStream: DOS on CRI

[high] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.5.0

SpdyStream: DOS on CRI

[high] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[high] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[high] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[high] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS

[high] CVE-2026-39883 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking

[high] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[high] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[high] CVE-2026-44973 — pkg:golang/github.com/go-git/go-billy/v5@v5.5.0

go-billy has path traversal vulnerabilities

[high] CVE-2026-44973 — pkg:golang/github.com/go-git/go-billy/v5@v5.6.2

go-billy has path traversal vulnerabilities

[high] CVE-2026-45022 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

[high] CVE-2026-45022 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

[high] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[high] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[high] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[high] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic

[high] CVE-2026-48702 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

[high] CVE-2026-48702 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

[high] CVE-2026-49478 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

[high] CVE-2026-49478 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

[high] CVE-2026-50163 — pkg:golang/oras.land/oras-go/v2@v2.6.1

`oras-go` tar extraction: Hardlink entry with relative Linkname escapes extract dir via process CWD resolution

[high] CVE-2026-53488 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

[high] CVE-2026-53488 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

[high] CVE-2026-54167 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

[high] CVE-2026-54167 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header

[high] CVE-2026-71556 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Worktree operations may follow symlinks

[high] CVE-2026-71556 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Worktree operations may follow symlinks

[high] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[high] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[high] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[high] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.79.3

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[high] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.80.0

gRPC-Go: Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation

[high] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[high] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[high] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[high] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.79.3

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[high] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.80.0

gRPC-Go xDS servers: Denial of Service (DoS) via crash due to missing `:authority` and `Host` headers

[high] CVE-2026-85731 — pkg:golang/oras.land/oras-go/v2@v2.6.1

oras-go: Arbitrary file write outside file.Store root via symlink-chain bypass in tar extraction (pushDir)

[high] CVE-2026-9804 — pkg:golang/kubevirt.io/kubevirt

KubeVirt has a Link Following issue

[high] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[high] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[high] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[high] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.79.3

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[high] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.80.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

[high] GHSA-q382-vc8q-7jhj — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

[medium] CVE-2020-1701 — pkg:golang/kubevirt.io/kubevirt

Permissions bypass in KubeVirt

[medium] CVE-2021-21303 — pkg:golang/helm.sh/helm/v3

Improper Neutralization of Special Elements in Output in helm.sh/helm/v3

[medium] CVE-2021-32690 — pkg:golang/helm.sh/helm/v3

Helm passes repository credentials to alternate domain

[medium] CVE-2022-23524 — pkg:golang/helm.sh/helm/v3

Helm vulnerable to denial of service through string value parsing

[medium] CVE-2022-23525 — pkg:golang/helm.sh/helm/v3

Helm vulnerable to denial of service through through repository index file

[medium] CVE-2022-23526 — pkg:golang/helm.sh/helm/v3

Helm vulnerable to denial of service through schema file

[medium] CVE-2022-36055 — pkg:golang/helm.sh/helm/v3

Helm Vulnerable to denial of service through string value parsing

[medium] CVE-2023-25165 — pkg:golang/helm.sh/helm/v3

Helm vulnerable to information disclosure via getHostByName Function

[medium] CVE-2023-45288 — pkg:golang/net/http?type=package

net/http, x/net/http2: close connections when receiving too many headers

[medium] CVE-2024-25620 — pkg:golang/helm.sh/helm/v3

Helm dependency management path traversal

[medium] CVE-2024-31420 — pkg:golang/kubevirt.io/kubevirt

KubeVirt NULL pointer dereference flaw

[medium] CVE-2024-33394 — pkg:golang/kubevirt.io/kubevirt

kubevirt allows a local attacker to execute arbitrary code via a crafted command

[medium] CVE-2024-40635 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd has an integer overflow in User ID handling

[medium] CVE-2024-45310 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc can be confused to create empty files/directories on the host

[medium] CVE-2024-45339 — pkg:golang/github.com/golang/glog

Insecure Temporary File usage in github.com/golang/glog

[medium] CVE-2024-45339 — pkg:golang/github.com/golang/glog@v1.2.2

Insecure Temporary File usage in github.com/golang/glog

[medium] CVE-2025-14525 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Guest Agent DoS via Excessive Network Interface Reports

[medium] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[medium] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.34.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[medium] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[medium] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.33.0

golang.org/x/net vulnerable to Cross-site Scripting

[medium] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.34.0

golang.org/x/net vulnerable to Cross-site Scripting

[medium] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.35.0

golang.org/x/net vulnerable to Cross-site Scripting

[medium] CVE-2025-27144 — pkg:golang/github.com/go-jose/go-jose/v3@v3.0.3

DoS in go-jose Parsing

[medium] CVE-2025-32386 — pkg:golang/helm.sh/helm/v3

Helm Allows A Specially Crafted Chart Archive To Cause Out Of Memory Termination

[medium] CVE-2025-32387 — pkg:golang/helm.sh/helm/v3

Helm Allows A Specially Crafted JSON Schema To Cause A Stack Overflow

[medium] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

[medium] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

[medium] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

[medium] CVE-2025-55198 — pkg:golang/helm.sh/helm/v3

Helm May Panic Due To Incorrect YAML Content

[medium] CVE-2025-55199 — pkg:golang/helm.sh/helm/v3

Helm Charts with Specific JSON Schema Values Can Cause Memory Exhaustion

[medium] CVE-2025-58058 — pkg:golang/github.com/ulikunitz/xz@v0.5.11

github.com/ulikunitz/xz leaks memory when decoding a corrupted multiple LZMA archives

[medium] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

[medium] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

[medium] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

[medium] CVE-2025-64329 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI server: Host memory exhaustion through Attach goroutine leak

[medium] CVE-2025-64432 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Affected by an Authentication Bypass in Kubernetes Aggregation Layer

[medium] CVE-2025-64433 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Arbitrary Container File Read

[medium] CVE-2025-64434 — pkg:golang/kubevirt.io/kubevirt

KubeVirt's Improper TLS Certificate Management Handling Allows API Identity Spoofing

[medium] CVE-2025-64435 — pkg:golang/kubevirt.io/kubevirt

KubeVirt VMI Denial-of-Service (DoS) Using Pod Impersonation

[medium] CVE-2025-64436 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Excessive Role Permissions Could Enable Unauthorized VMI Migrations Between Nodes

[medium] CVE-2025-64437 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Isolation Detection Flaw Allows Arbitrary File Permission Changes

[medium] CVE-2025-71405 — pkg:golang/github.com/go-chi/chi/v5@v5.1.0

chi Allows Host Header Injection which Leads to Open Redirect in RedirectSlashes

[medium] CVE-2026-22703 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions

[medium] CVE-2026-22772 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

[medium] CVE-2026-22772 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

[medium] CVE-2026-2303 — pkg:golang/go.mongodb.org/mongo-driver@v1.14.0

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

[medium] CVE-2026-2303 — pkg:golang/go.mongodb.org/mongo-driver@v1.16.1

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

[medium] CVE-2026-23831 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

[medium] CVE-2026-23831 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

[medium] CVE-2026-23991 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf affected by client DoS via malformed server response

[medium] CVE-2026-23992 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf improperly validates the configured threshold for delegations

[medium] CVE-2026-24117 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

[medium] CVE-2026-24117 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

[medium] CVE-2026-24137 — pkg:golang/github.com/sigstore/sigstore@v1.8.15

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

[medium] CVE-2026-24137 — pkg:golang/github.com/sigstore/sigstore@v1.8.2

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

[medium] CVE-2026-24686 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf Path Traversal in TAP 4 Multirepo Client Allows Arbitrary File Write via Malicious Repository Names

[medium] CVE-2026-25542 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

[medium] CVE-2026-25542 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

[medium] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.33.0

Go Net HTML parser is vulnerable to denial of service

[medium] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.34.0

Go Net HTML parser is vulnerable to denial of service

[medium] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.35.0

Go Net HTML parser is vulnerable to denial of service

[medium] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.41.0

Go Net HTML parser is vulnerable to denial of service

[medium] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.52.0

Go Net HTML parser is vulnerable to denial of service

[medium] CVE-2026-25934 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git improperly verifies data integrity values for .idx and .pack files

[medium] CVE-2026-25934 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git improperly verifies data integrity values for .idx and .pack files

[medium] CVE-2026-33022 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

[medium] CVE-2026-33022 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

[medium] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Moby has an Off-by-one error in its plugin privilege validation

[medium] CVE-2026-34165 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

[medium] CVE-2026-34165 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

[medium] CVE-2026-35206 — pkg:golang/helm.sh/helm/v3

Helm Chart extraction output directory collapse via `Chart.yaml` name dot-segment

[medium] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[medium] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[medium] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[medium] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS

[medium] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[medium] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[medium] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[medium] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

[medium] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[medium] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[medium] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[medium] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow

[medium] CVE-2026-41506 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Credential leak via cross-host redirect in smart HTTP transport

[medium] CVE-2026-41506 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Credential leak via cross-host redirect in smart HTTP transport

[medium] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[medium] CVE-2026-41579 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc: Malicious image with /dev symlink can trigger limited host filesystem integrity violations

[medium] CVE-2026-41888 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution's tag deletion bypasses `storage.delete.enabled` configuration

[medium] CVE-2026-44740 — pkg:golang/github.com/go-git/go-billy/v5@v5.5.0

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

[medium] CVE-2026-44740 — pkg:golang/github.com/go-git/go-billy/v5@v5.6.2

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

[medium] CVE-2026-45571 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Crafted repositories may modify main and submodule .git directories

[medium] CVE-2026-45571 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Crafted repositories may modify main and submodule .git directories

[medium] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[medium] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[medium] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[medium] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic

[medium] CVE-2026-47262 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd image-triggered runtime DoS via unbounded group parsing

[medium] CVE-2026-47262 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd image-triggered runtime DoS via unbounded group parsing

[medium] CVE-2026-49834 — pkg:golang/github.com/sigstore/sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log

[medium] CVE-2026-49835 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality

[medium] CVE-2026-53495 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service

[medium] CVE-2026-53495 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service

[medium] CVE-2026-54168 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

[medium] CVE-2026-54168 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution

[medium] CVE-2026-61711 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit: Custom frontend could bypass Seccomp/AppArmor

[medium] CVE-2026-61711 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit: Custom frontend could bypass Seccomp/AppArmor

[medium] CVE-2026-6383 — pkg:golang/kubevirt.io/kubevirt

KubeVirt's authorization mechanism improperly truncates subresource names

[medium] CVE-2026-71557 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Malicious reference names may modify files outside the reference storage

[medium] CVE-2026-71557 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Malicious reference names may modify files outside the reference storage

[medium] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[medium] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[medium] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[medium] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.79.3

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[medium] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.80.0

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[medium] CVE-2026-85732 — pkg:golang/oras.land/oras-go/v2@v2.6.1

oras-go: Blind SSRF via unvalidated Link header URL in pagination allows internal network probing

[medium] CVE-2026-89090 — pkg:golang/github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream@v1.6.8

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

[medium] CVE-2026-89090 — pkg:golang/github.com/aws/aws-sdk-go-v2/service/s3@v1.76.0

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

[medium] GHSA-gcjh-h69q-9w9g — pkg:golang/github.com/google/cel-go@v0.23.2

cel-go: JSON Private Fields Exposed via NativeTypes and ParseStructTag

[medium] GHSA-pmwq-pjrm-6p5r — pkg:golang/github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior

[medium] GHSA-w5pp-99ch-qj29 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Malformed Git object data may cause panics or resource exhaustion

[medium] GHSA-w5pp-99ch-qj29 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Malformed Git object data may cause panics or resource exhaustion

[medium] GHSA-w67g-5rqw-f597 — pkg:golang/github.com/gorilla/websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

[medium] GHSA-w67g-5rqw-f597 — pkg:golang/github.com/gorilla/websocket@v1.5.0?type=module

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

[medium] GHSA-w67g-5rqw-f597 — pkg:golang/github.com/gorilla/websocket@v1.5.0?type=package

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key

[low] CVE-2020-15184 — pkg:golang/helm.sh/helm/v3

Aliases are never checked in helm

[low] CVE-2020-15185 — pkg:golang/helm.sh/helm/v3

Repository index file allows for duplicates of the same chart entry in helm

[low] CVE-2020-15186 — pkg:golang/helm.sh/helm/v3

Improper Sanitizing of plugin names in helm

[low] CVE-2020-15187 — pkg:golang/helm.sh/helm/v3

plugin.yaml file allows for duplicate entries in helm

[low] CVE-2020-4053 — pkg:golang/helm.sh/helm/v3

Plugin archive directory traversal in Helm

[low] CVE-2025-54410 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Moby firewalld reload removes bridge network isolation

[low] CVE-2025-54410 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Moby firewalld reload removes bridge network isolation

[low] CVE-2025-8556 — pkg:golang/github.com/cloudflare/circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results

[low] CVE-2026-1229 — pkg:golang/github.com/cloudflare/circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult

[low] CVE-2026-1229 — pkg:golang/github.com/cloudflare/circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult

[low] CVE-2026-33762 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git missing validation decoding Index v4 files leads to panic

[low] CVE-2026-33762 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git missing validation decoding Index v4 files leads to panic

[low] CVE-2026-45570 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Improper single-quote escaping in go-git SSH transport

[low] CVE-2026-45570 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Improper single-quote escaping in go-git SSH transport

[low] CVE-2026-54787 — pkg:golang/github.com/sigstore/sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period

[low] CVE-2026-61712 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit has a possible runtime DoS via unbounded group parsing

[low] CVE-2026-61712 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit has a possible runtime DoS via unbounded group parsing

[low] CVE-2026-81870 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry-Go: Exporter config logging may leak endpoint URLs in info logs

[unknown] CVE-2020-14316 — pkg:golang/kubevirt.io/kubevirt

Privilege Escalation in kubevirt in kubevirt.io/kubevirt

[unknown] CVE-2020-1701 — pkg:golang/kubevirt.io/kubevirt

Permissions bypass in KubeVirt in kubevirt.io/kubevirt

[unknown] CVE-2020-8911 — pkg:golang/github.com/aws/aws-sdk-go@v1.53.12

CBC padding oracle issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2020-8911 — pkg:golang/github.com/aws/aws-sdk-go@v1.55.6

CBC padding oracle issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2020-8912 — pkg:golang/github.com/aws/aws-sdk-go@v1.53.12

In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2020-8912 — pkg:golang/github.com/aws/aws-sdk-go@v1.55.6

In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2021-21303 — pkg:golang/helm.sh/helm/v3

Insufficient sanitization of data files in helm.sh/helm/v3

[unknown] CVE-2021-32690 — pkg:golang/helm.sh/helm/v3

Repository credentials passed to alternate domain in helm.sh/helm/v3

[unknown] CVE-2022-23524 — pkg:golang/helm.sh/helm/v3

Denial of service in string value parsing in helm.sh/helm/v3

[unknown] CVE-2022-23525 — pkg:golang/helm.sh/helm/v3

Denial of service via repository index file in helm.sh/helm/v3

[unknown] CVE-2022-23526 — pkg:golang/helm.sh/helm/v3

Denial of service via schema file in helm.sh/helm/v3

[unknown] CVE-2022-36055 — pkg:golang/helm.sh/helm/v3

Denial of service through string value parsing in helm.sh/helm/v3

[unknown] CVE-2023-25165 — pkg:golang/helm.sh/helm/v3

Information disclosure in helm.sh/helm/v3

[unknown] CVE-2023-37264 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Pipelines do not validate child UIDs in github.com/tektoncd/pipeline

[unknown] CVE-2023-37264 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Pipelines do not validate child UIDs in github.com/tektoncd/pipeline

[unknown] CVE-2024-25620 — pkg:golang/helm.sh/helm/v3

Path traversal in helm.sh/helm/v3

[unknown] CVE-2024-25621 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd affected by a local privilege escalation via wide permissions on CRI directory in github.com/containerd/containerd

[unknown] CVE-2024-26147 — pkg:golang/helm.sh/helm/v3

Helm's Missing YAML Content Leads To Panic in helm.sh/helm/v3

[unknown] CVE-2024-31420 — pkg:golang/kubevirt.io/kubevirt

KubeVirt NULL pointer dereference flaw in kubevirt.io/kubevirt

[unknown] CVE-2024-33394 — pkg:golang/kubevirt.io/kubevirt

kubevirt allows a local attacker to execute arbitrary code via a crafted command in kubevirt.io/kubevirt

[unknown] CVE-2024-40635 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd has an integer overflow in User ID handling in github.com/containerd/containerd

[unknown] CVE-2024-45310 — pkg:golang/github.com/opencontainers/runc@v1.1.12

Can be confused to create empty files/directories on the host in github.com/opencontainers/runc

[unknown] CVE-2024-45339 — pkg:golang/github.com/golang/glog

Vulnerability when creating log files in github.com/golang/glog

[unknown] CVE-2024-45339 — pkg:golang/github.com/golang/glog@v1.2.2

Vulnerability when creating log files in github.com/golang/glog

[unknown] CVE-2024-5042 — pkg:golang/github.com/submariner-io/submariner-operator@v0.24.0

Submariner Operator sets unnecessary RBAC permissions in helm charts in github.com/submariner-io/submariner-operator

[unknown] CVE-2025-0913 — pkg:golang/stdlib@1.22.12

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

[unknown] CVE-2025-0913 — pkg:golang/stdlib@1.23.6

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

[unknown] CVE-2025-14525 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Guest Agent DoS via Excessive Network Interface Reports in kubevirt.io/kubevirt

[unknown] CVE-2025-15558 — pkg:golang/github.com/docker/cli@v27.4.1%2Bincompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows in github.com/docker/cli

[unknown] CVE-2025-15558 — pkg:golang/github.com/docker/cli@v28.0.0%2Bincompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows in github.com/docker/cli

[unknown] CVE-2025-21613 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Argument Injection via the URL field in github.com/go-git/go-git

[unknown] CVE-2025-21614 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Clients vulnerable to DoS via maliciously crafted Git server replies in github.com/go-git/go-git

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.12.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.18.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.23.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.26.0

Unexpected memory consumption during token parsing in golang.org/x/oauth2

[unknown] CVE-2025-22869 — pkg:golang/golang.org/x/crypto@v0.32.0

Potential denial of service in golang.org/x/crypto

[unknown] CVE-2025-22869 — pkg:golang/golang.org/x/crypto@v0.33.0

Potential denial of service in golang.org/x/crypto

[unknown] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.34.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] CVE-2025-22870 — pkg:golang/stdlib@1.22.12

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] CVE-2025-22870 — pkg:golang/stdlib@1.23.6

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] CVE-2025-22871 — pkg:golang/stdlib@1.22.12

Request smuggling due to acceptance of invalid chunked data in net/http

[unknown] CVE-2025-22871 — pkg:golang/stdlib@1.23.6

Request smuggling due to acceptance of invalid chunked data in net/http

[unknown] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.33.0

Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

[unknown] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.34.0

Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

[unknown] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.35.0

Incorrect Neutralization of Input During Web Page Generation in x/net in golang.org/x/net

[unknown] CVE-2025-22873 — pkg:golang/stdlib@1.22.12

Improper access to parent directory of root in os

[unknown] CVE-2025-22873 — pkg:golang/stdlib@1.23.6

Improper access to parent directory of root in os

[unknown] CVE-2025-27144 — pkg:golang/github.com/go-jose/go-jose/v3@v3.0.3

DoS in go-jose Parsing in github.com/go-jose/go-jose

[unknown] CVE-2025-30204 — pkg:golang/github.com/golang-jwt/jwt/v4@v4.5.1

Excessive memory allocation during header parsing in github.com/golang-jwt/jwt

[unknown] CVE-2025-30204 — pkg:golang/github.com/golang-jwt/jwt/v5@v5.2.1

Excessive memory allocation during header parsing in github.com/golang-jwt/jwt

[unknown] CVE-2025-31133 — pkg:golang/github.com/opencontainers/runc@v1.1.12

Container escape via "masked path" abuse due to mount race conditions in github.com/opencontainers/runc

[unknown] CVE-2025-32386 — pkg:golang/helm.sh/helm/v3

Helm Allows A Specially Crafted Chart Archive To Cause Out Of Memory Termination in helm.sh/helm

[unknown] CVE-2025-32387 — pkg:golang/helm.sh/helm/v3

Helm Allows A Specially Crafted JSON Schema To Cause A Stack Overflow in helm.sh/helm

[unknown] CVE-2025-4673 — pkg:golang/stdlib@1.22.12

Sensitive headers not cleared on cross-origin redirect in net/http

[unknown] CVE-2025-4673 — pkg:golang/stdlib@1.23.6

Sensitive headers not cleared on cross-origin redirect in net/http

[unknown] CVE-2025-47906 — pkg:golang/stdlib@1.22.12

Unexpected paths returned from LookPath in os/exec

[unknown] CVE-2025-47906 — pkg:golang/stdlib@1.23.6

Unexpected paths returned from LookPath in os/exec

[unknown] CVE-2025-47907 — pkg:golang/stdlib@1.22.12

Incorrect results returned from Rows.Scan in database/sql

[unknown] CVE-2025-47907 — pkg:golang/stdlib@1.23.6

Incorrect results returned from Rows.Scan in database/sql

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.33.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.34.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.35.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.41.0

Quadratic parsing complexity in golang.org/x/net/html

[unknown] CVE-2025-47912 — pkg:golang/stdlib@1.22.12

Insufficient validation of bracketed IPv6 hostnames in net/url

[unknown] CVE-2025-47912 — pkg:golang/stdlib@1.23.6

Insufficient validation of bracketed IPv6 hostnames in net/url

[unknown] CVE-2025-47913 — pkg:golang/golang.org/x/crypto@v0.32.0

Potential denial of service in golang.org/x/crypto/ssh/agent

[unknown] CVE-2025-47913 — pkg:golang/golang.org/x/crypto@v0.33.0

Potential denial of service in golang.org/x/crypto/ssh/agent

[unknown] CVE-2025-47913 — pkg:golang/golang.org/x/crypto@v0.39.0

Potential denial of service in golang.org/x/crypto/ssh/agent

[unknown] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.32.0

Malformed constraint may cause denial of service in golang.org/x/crypto/ssh/agent

[unknown] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.33.0

Malformed constraint may cause denial of service in golang.org/x/crypto/ssh/agent

[unknown] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.39.0

Malformed constraint may cause denial of service in golang.org/x/crypto/ssh/agent

[unknown] CVE-2025-52565 — pkg:golang/github.com/opencontainers/runc@v1.1.12

Container escape with malicious config due to /dev/console mount and related races in github.com/opencontainers/runc

[unknown] CVE-2025-52881 — pkg:golang/github.com/opencontainers/runc@v1.1.12

Container escape and DDoS due to arbitrary write gadgets and procfs write redirects in github.com/opencontainers/runc

[unknown] CVE-2025-52881 — pkg:golang/github.com/opencontainers/selinux@v1.11.0

Container escape and DDoS due to arbitrary write gadgets and procfs write redirects in github.com/opencontainers/runc

[unknown] CVE-2025-53547 — pkg:golang/helm.sh/helm/v3

Helm vulnerable to Code Injection through malicious chart.yaml content in helm.sh/helm

[unknown] CVE-2025-54410 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Moby firewalld reload removes bridge network isolation in github.com/docker/docker

[unknown] CVE-2025-55198 — pkg:golang/helm.sh/helm/v3

Helm May Panic Due To Incorrect YAML Content in helm.sh/helm

[unknown] CVE-2025-55199 — pkg:golang/helm.sh/helm/v3

Helm Charts with Specific JSON Schema Values Can Cause Memory Exhaustion in helm.sh/helm

[unknown] CVE-2025-58058 — pkg:golang/github.com/ulikunitz/xz@v0.5.11

Memory leaks when decoding a corrupted multiple LZMA archives in github.com/ulikunitz/xz

[unknown] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.32.0

Unbounded memory consumption in golang.org/x/crypto/ssh

[unknown] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.33.0

Unbounded memory consumption in golang.org/x/crypto/ssh

[unknown] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.39.0

Unbounded memory consumption in golang.org/x/crypto/ssh

[unknown] CVE-2025-58183 — pkg:golang/stdlib@1.22.12

Unbounded allocation when parsing GNU sparse map in archive/tar

[unknown] CVE-2025-58183 — pkg:golang/stdlib@1.23.6

Unbounded allocation when parsing GNU sparse map in archive/tar

[unknown] CVE-2025-58185 — pkg:golang/stdlib@1.22.12

Parsing DER payload can cause memory exhaustion in encoding/asn1

[unknown] CVE-2025-58185 — pkg:golang/stdlib@1.23.6

Parsing DER payload can cause memory exhaustion in encoding/asn1

[unknown] CVE-2025-58186 — pkg:golang/stdlib@1.22.12

Lack of limit when parsing cookies can cause memory exhaustion in net/http

[unknown] CVE-2025-58186 — pkg:golang/stdlib@1.23.6

Lack of limit when parsing cookies can cause memory exhaustion in net/http

[unknown] CVE-2025-58187 — pkg:golang/stdlib@1.22.12

Quadratic complexity when checking name constraints in crypto/x509

[unknown] CVE-2025-58187 — pkg:golang/stdlib@1.23.6

Quadratic complexity when checking name constraints in crypto/x509

[unknown] CVE-2025-58188 — pkg:golang/stdlib@1.22.12

Panic when validating certificates with DSA public keys in crypto/x509

[unknown] CVE-2025-58188 — pkg:golang/stdlib@1.23.6

Panic when validating certificates with DSA public keys in crypto/x509

[unknown] CVE-2025-58189 — pkg:golang/stdlib@1.22.12

ALPN negotiation error contains attacker controlled information in crypto/tls

[unknown] CVE-2025-58189 — pkg:golang/stdlib@1.23.6

ALPN negotiation error contains attacker controlled information in crypto/tls

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.33.0

Infinite parsing loop in golang.org/x/net

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.34.0

Infinite parsing loop in golang.org/x/net

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.35.0

Infinite parsing loop in golang.org/x/net

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.41.0

Infinite parsing loop in golang.org/x/net

[unknown] CVE-2025-61723 — pkg:golang/stdlib@1.22.12

Quadratic complexity when parsing some invalid inputs in encoding/pem

[unknown] CVE-2025-61723 — pkg:golang/stdlib@1.23.6

Quadratic complexity when parsing some invalid inputs in encoding/pem

[unknown] CVE-2025-61724 — pkg:golang/stdlib@1.22.12

Excessive CPU consumption in Reader.ReadResponse in net/textproto

[unknown] CVE-2025-61724 — pkg:golang/stdlib@1.23.6

Excessive CPU consumption in Reader.ReadResponse in net/textproto

[unknown] CVE-2025-61725 — pkg:golang/stdlib@1.22.12

Excessive CPU consumption in ParseAddress in net/mail

[unknown] CVE-2025-61725 — pkg:golang/stdlib@1.23.6

Excessive CPU consumption in ParseAddress in net/mail

[unknown] CVE-2025-61726 — pkg:golang/stdlib@1.22.12

Memory exhaustion in query parameter parsing in net/url

[unknown] CVE-2025-61726 — pkg:golang/stdlib@1.23.6

Memory exhaustion in query parameter parsing in net/url

[unknown] CVE-2025-61726 — pkg:golang/stdlib@1.25.5

Memory exhaustion in query parameter parsing in net/url

[unknown] CVE-2025-61727 — pkg:golang/stdlib@1.22.12

Improper application of excluded DNS name constraints when verifying wildcard names in crypto/x509

[unknown] CVE-2025-61727 — pkg:golang/stdlib@1.23.6

Improper application of excluded DNS name constraints when verifying wildcard names in crypto/x509

[unknown] CVE-2025-61728 — pkg:golang/stdlib@1.22.12

Excessive CPU consumption when building archive index in archive/zip

[unknown] CVE-2025-61728 — pkg:golang/stdlib@1.23.6

Excessive CPU consumption when building archive index in archive/zip

[unknown] CVE-2025-61728 — pkg:golang/stdlib@1.25.5

Excessive CPU consumption when building archive index in archive/zip

[unknown] CVE-2025-61729 — pkg:golang/stdlib@1.22.12

Excessive resource consumption when printing error string for host certificate validation in crypto/x509

[unknown] CVE-2025-61729 — pkg:golang/stdlib@1.23.6

Excessive resource consumption when printing error string for host certificate validation in crypto/x509

[unknown] CVE-2025-61730 — pkg:golang/stdlib@1.22.12

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] CVE-2025-61730 — pkg:golang/stdlib@1.23.6

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] CVE-2025-61730 — pkg:golang/stdlib@1.25.5

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] CVE-2025-64324 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Vulnerable to Arbitrary Host File Read and Write in kubevirt.io/kubevirt

[unknown] CVE-2025-64329 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI server: Host memory exhaustion through Attach goroutine leak in github.com/containerd/containerd

[unknown] CVE-2025-64432 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Affected by an Authentication Bypass in Kubernetes Aggregation Layer in kubevirt.io/kubevirt

[unknown] CVE-2025-64433 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Arbitrary Container File Read in kubevirt.io/kubevirt

[unknown] CVE-2025-64434 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Improper TLS Certificate Management Handling Allows API Identity Spoofing in kubevirt.io/kubevirt

[unknown] CVE-2025-64435 — pkg:golang/kubevirt.io/kubevirt

KubeVirt VMI Denial-of-Service (DoS) Using Pod Impersonation in kubevirt.io/kubevirt

[unknown] CVE-2025-64437 — pkg:golang/kubevirt.io/kubevirt

KubeVirt Isolation Detection Flaw Allows Arbitrary File Permission Changes in kubevirt.io/kubevirt

[unknown] CVE-2025-66506 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio allocates excessive memory during token parsing in github.com/sigstore/fulcio

[unknown] CVE-2025-66506 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing in github.com/sigstore/fulcio

[unknown] CVE-2025-66564 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing in github.com/sigstore/timestamp-authority

[unknown] CVE-2025-68121 — pkg:golang/stdlib@1.22.12

Unexpected session resumption in crypto/tls

[unknown] CVE-2025-68121 — pkg:golang/stdlib@1.23.6

Unexpected session resumption in crypto/tls

[unknown] CVE-2025-68121 — pkg:golang/stdlib@1.25.5

Unexpected session resumption in crypto/tls

[unknown] CVE-2025-69725 — pkg:golang/github.com/go-chi/chi@v4.1.2%2Bincompatible

Open redirect vulnerability in the RedirectSlashes middleware in github.com/go-chi/chi

[unknown] CVE-2025-8556 — pkg:golang/github.com/cloudflare/circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results in github.com/cloudflare/circl

[unknown] CVE-2026-1229 — pkg:golang/github.com/cloudflare/circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult in github.com/cloudflare/circl

[unknown] CVE-2026-1229 — pkg:golang/github.com/cloudflare/circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult in github.com/cloudflare/circl

[unknown] CVE-2026-22703 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions in github.com/sigstore/cosign

[unknown] CVE-2026-22772 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass in github.com/sigstore/fulcio

[unknown] CVE-2026-22772 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass in github.com/sigstore/fulcio

[unknown] CVE-2026-2303 — pkg:golang/go.mongodb.org/mongo-driver@v1.14.0

Mongo-go-driver: Heap Out-of-Bounds Read in GSSAPI Error Handling in go.mongodb.org/mongo-driver

[unknown] CVE-2026-2303 — pkg:golang/go.mongodb.org/mongo-driver@v1.16.1

Mongo-go-driver: Heap Out-of-Bounds Read in GSSAPI Error Handling in go.mongodb.org/mongo-driver

[unknown] CVE-2026-23831 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message in github.com/sigstore/rekor

[unknown] CVE-2026-23831 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message in github.com/sigstore/rekor

[unknown] CVE-2026-23991 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

Client DoS via malformed server response in github.com/theupdateframework/go-tuf

[unknown] CVE-2026-23992 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

Improper validattion of configured threshold for delegations in github.com/theupdateframework/go-tuf

[unknown] CVE-2026-24051 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking in go.opentelemetry.io/otel/sdk

[unknown] CVE-2026-24117 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL in github.com/sigstore/rekor

[unknown] CVE-2026-24117 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL in github.com/sigstore/rekor

[unknown] CVE-2026-24122 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign considered signatures valid with expired intermediate certificates when transparency log verification is skipped in github.com/sigstore/cosign

[unknown] CVE-2026-24137 — pkg:golang/github.com/sigstore/sigstore@v1.8.15

Sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal in github.com/sigstore/sigstore

[unknown] CVE-2026-24137 — pkg:golang/github.com/sigstore/sigstore@v1.8.2

Sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal in github.com/sigstore/sigstore

[unknown] CVE-2026-24686 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

Path traversal in TAP 4 multirepo client allows arbitrary file write via repo names in github.com/theupdateframework/go-tuf

[unknown] CVE-2026-25542 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching in github.com/tektoncd/pipeline

[unknown] CVE-2026-25542 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching in github.com/tektoncd/pipeline

[unknown] CVE-2026-25679 — pkg:golang/stdlib@1.22.12

Incorrect parsing of IPv6 host literals in net/url

[unknown] CVE-2026-25679 — pkg:golang/stdlib@1.23.6

Incorrect parsing of IPv6 host literals in net/url

[unknown] CVE-2026-25679 — pkg:golang/stdlib@1.25.5

Incorrect parsing of IPv6 host literals in net/url

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.33.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.34.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.35.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.41.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.52.0

Invoking denial of service when parsing arbitrary HTML in golang.org/x/net/html

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.33.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.34.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.35.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.41.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.52.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

[unknown] CVE-2026-25934 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Improper verification of data integrity values for .idx and .pack files in github.com/go-git/go-git

[unknown] CVE-2026-25934 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Improper verification of data integrity values for .idx and .pack files in github.com/go-git/go-git

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.33.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.34.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.35.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.41.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.52.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

[unknown] CVE-2026-27139 — pkg:golang/stdlib@1.22.12

FileInfo can escape from a Root in os

[unknown] CVE-2026-27139 — pkg:golang/stdlib@1.23.6

FileInfo can escape from a Root in os

[unknown] CVE-2026-27139 — pkg:golang/stdlib@1.25.5

FileInfo can escape from a Root in os

[unknown] CVE-2026-27142 — pkg:golang/stdlib@1.22.12

URLs in meta content attribute actions are not escaped in html/template

[unknown] CVE-2026-27142 — pkg:golang/stdlib@1.23.6

URLs in meta content attribute actions are not escaped in html/template

[unknown] CVE-2026-27142 — pkg:golang/stdlib@1.25.5

URLs in meta content attribute actions are not escaped in html/template

[unknown] CVE-2026-27145 — pkg:golang/stdlib@1.22.12

Inefficient candidate hostname parsing in crypto/x509

[unknown] CVE-2026-27145 — pkg:golang/stdlib@1.23.6

Inefficient candidate hostname parsing in crypto/x509

[unknown] CVE-2026-27145 — pkg:golang/stdlib@1.25.5

Inefficient candidate hostname parsing in crypto/x509

[unknown] CVE-2026-27145 — pkg:golang/stdlib@1.25.9

Inefficient candidate hostname parsing in crypto/x509

[unknown] CVE-2026-27145 — pkg:golang/stdlib@1.26.2

Inefficient candidate hostname parsing in crypto/x509

[unknown] CVE-2026-27896 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

MCP Go SDK Vulnerable to Improper Handling of Case Sensitivity in github.com/modelcontextprotocol/go-sdk

[unknown] CVE-2026-32280 — pkg:golang/stdlib@1.22.12

Unexpected work during chain building in crypto/x509

[unknown] CVE-2026-32280 — pkg:golang/stdlib@1.23.6

Unexpected work during chain building in crypto/x509

[unknown] CVE-2026-32280 — pkg:golang/stdlib@1.25.5

Unexpected work during chain building in crypto/x509

[unknown] CVE-2026-32281 — pkg:golang/stdlib@1.22.12

Inefficient policy validation in crypto/x509

[unknown] CVE-2026-32281 — pkg:golang/stdlib@1.23.6

Inefficient policy validation in crypto/x509

[unknown] CVE-2026-32281 — pkg:golang/stdlib@1.25.5

Inefficient policy validation in crypto/x509

[unknown] CVE-2026-32282 — pkg:golang/stdlib@1.22.12

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] CVE-2026-32282 — pkg:golang/stdlib@1.23.6

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] CVE-2026-32282 — pkg:golang/stdlib@1.25.5

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] CVE-2026-32283 — pkg:golang/stdlib@1.22.12

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] CVE-2026-32283 — pkg:golang/stdlib@1.23.6

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] CVE-2026-32283 — pkg:golang/stdlib@1.25.5

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] CVE-2026-32288 — pkg:golang/stdlib@1.22.12

Unbounded allocation for old GNU sparse in archive/tar

[unknown] CVE-2026-32288 — pkg:golang/stdlib@1.23.6

Unbounded allocation for old GNU sparse in archive/tar

[unknown] CVE-2026-32288 — pkg:golang/stdlib@1.25.5

Unbounded allocation for old GNU sparse in archive/tar

[unknown] CVE-2026-32289 — pkg:golang/stdlib@1.22.12

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] CVE-2026-32289 — pkg:golang/stdlib@1.23.6

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] CVE-2026-32289 — pkg:golang/stdlib@1.25.5

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] CVE-2026-33022 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun in github.com/tektoncd/pipeline

[unknown] CVE-2026-33022 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun in github.com/tektoncd/pipeline

[unknown] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.67.1

Authorization bypass in gRPC-Go via missing leading slash in :path in google.golang.org/grpc

[unknown] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.69.4

Authorization bypass in gRPC-Go via missing leading slash in :path in google.golang.org/grpc

[unknown] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.70.0

Authorization bypass in gRPC-Go via missing leading slash in :path in google.golang.org/grpc

[unknown] CVE-2026-33252 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Cross-Site Tool Execution for HTTP Servers without Authorizatrion in github.com/modelcontextprotocol/go-sdk

[unknown] CVE-2026-33540 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution affected by pull-through cache credential exfiltration via www-authenticate bearer realm in github.com/distribution/distribution

[unknown] CVE-2026-33747 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit's Malicious frontend can cause file escape outside of storage root in github.com/moby/buildkit

[unknown] CVE-2026-33747 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit's Malicious frontend can cause file escape outside of storage root in github.com/moby/buildkit

[unknown] CVE-2026-33748 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit Git URL subdir component can cause access to restricted files in github.com/moby/buildkit

[unknown] CVE-2026-33748 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit Git URL subdir component can cause access to restricted files in github.com/moby/buildkit

[unknown] CVE-2026-33762 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Missing validation decoding Index v4 files leads to panic in github.com/go-git/go-git

[unknown] CVE-2026-33762 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Missing validation decoding Index v4 files leads to panic in github.com/go-git/go-git

[unknown] CVE-2026-33811 — pkg:golang/stdlib@1.22.12

Crash when handling long CNAME response in net

[unknown] CVE-2026-33811 — pkg:golang/stdlib@1.23.6

Crash when handling long CNAME response in net

[unknown] CVE-2026-33811 — pkg:golang/stdlib@1.25.5

Crash when handling long CNAME response in net

[unknown] CVE-2026-33811 — pkg:golang/stdlib@1.25.9

Crash when handling long CNAME response in net

[unknown] CVE-2026-33811 — pkg:golang/stdlib@1.26.2

Crash when handling long CNAME response in net

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.33.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.34.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.35.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.41.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.52.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/stdlib@1.22.12

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/stdlib@1.23.6

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/stdlib@1.25.5

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/stdlib@1.25.9

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33814 — pkg:golang/stdlib@1.26.2

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

[unknown] CVE-2026-33818 — pkg:golang/stdlib@1.22.12

Enforce maximum recursion depth in encoding/asn1

[unknown] CVE-2026-33818 — pkg:golang/stdlib@1.23.6

Enforce maximum recursion depth in encoding/asn1

[unknown] CVE-2026-33818 — pkg:golang/stdlib@1.25.5

Enforce maximum recursion depth in encoding/asn1

[unknown] CVE-2026-33818 — pkg:golang/stdlib@1.25.9

Enforce maximum recursion depth in encoding/asn1

[unknown] CVE-2026-33818 — pkg:golang/stdlib@1.26.2

Enforce maximum recursion depth in encoding/asn1

[unknown] CVE-2026-33818 — pkg:golang/stdlib@1.26.5

Enforce maximum recursion depth in encoding/asn1

[unknown] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Moby has an Off-by-one error in its plugin privilege validation in github.com/docker/docker

[unknown] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Moby has an Off-by-one error in its plugin privilege validation in github.com/docker/docker

[unknown] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Moby has an Off-by-one error in its plugin privilege validation in github.com/docker/docker

[unknown] CVE-2026-34040 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[unknown] CVE-2026-34040 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[unknown] CVE-2026-34040 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Moby has AuthZ plugin bypass when provided oversized request bodies in github.com/docker/docker

[unknown] CVE-2026-34165 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Maliciously crafted idx file can cause asymmetric memory consumption in github.com/go-git/go-git

[unknown] CVE-2026-34165 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Maliciously crafted idx file can cause asymmetric memory consumption in github.com/go-git/go-git

[unknown] CVE-2026-34742 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

DNS Rebinding Protection Disabled by Default in Model Context Protocol Go SDK for Servers Running on Localhost in github.com/modelcontextprotocol/go-sdk

[unknown] CVE-2026-34986 — pkg:golang/github.com/go-jose/go-jose/v3@v3.0.3

Go JOSE Panics in JWE decryption in github.com/go-jose/go-jose

[unknown] CVE-2026-34986 — pkg:golang/github.com/go-jose/go-jose/v4@v4.0.5

Go JOSE Panics in JWE decryption in github.com/go-jose/go-jose

[unknown] CVE-2026-35172 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Stale blob descriptor cache invalidation in github.com/distribution/distribution

[unknown] CVE-2026-35206 — pkg:golang/helm.sh/helm/v3

Helm Chart extraction output directory collapse via Chart.yaml name dot-segment in helm.sh/helm

[unknown] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.2.0

Uncontrolled resource consumption when parsing SPDY frames in github.com/moby/spdystream

[unknown] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.4.0

Uncontrolled resource consumption when parsing SPDY frames in github.com/moby/spdystream

[unknown] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.5.0

Uncontrolled resource consumption when parsing SPDY frames in github.com/moby/spdystream

[unknown] CVE-2026-39395 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign's verify-blob-attestation reports false positive when payload parsing fails in github.com/sigstore/cosign

[unknown] CVE-2026-39820 — pkg:golang/stdlib@1.22.12

Quadratic string concatentation in consumeComment in net/mail

[unknown] CVE-2026-39820 — pkg:golang/stdlib@1.23.6

Quadratic string concatentation in consumeComment in net/mail

[unknown] CVE-2026-39820 — pkg:golang/stdlib@1.25.5

Quadratic string concatentation in consumeComment in net/mail

[unknown] CVE-2026-39820 — pkg:golang/stdlib@1.25.9

Quadratic string concatentation in consumeComment in net/mail

[unknown] CVE-2026-39820 — pkg:golang/stdlib@1.26.2

Quadratic string concatentation in consumeComment in net/mail

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.33.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.34.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.35.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.41.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.52.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/stdlib@1.22.12

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/stdlib@1.23.6

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/stdlib@1.25.5

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/stdlib@1.25.9

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/stdlib@1.26.2

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39821 — pkg:golang/stdlib@1.26.5

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] CVE-2026-39822 — pkg:golang/stdlib@1.22.12

Root escape via symlink plus trailing slash in os

[unknown] CVE-2026-39822 — pkg:golang/stdlib@1.23.6

Root escape via symlink plus trailing slash in os

[unknown] CVE-2026-39822 — pkg:golang/stdlib@1.25.5

Root escape via symlink plus trailing slash in os

[unknown] CVE-2026-39822 — pkg:golang/stdlib@1.25.9

Root escape via symlink plus trailing slash in os

[unknown] CVE-2026-39822 — pkg:golang/stdlib@1.26.2

Root escape via symlink plus trailing slash in os

[unknown] CVE-2026-39823 — pkg:golang/stdlib@1.22.12

Bypass of meta content URL escaping causes XSS in html/template

[unknown] CVE-2026-39823 — pkg:golang/stdlib@1.23.6

Bypass of meta content URL escaping causes XSS in html/template

[unknown] CVE-2026-39823 — pkg:golang/stdlib@1.25.5

Bypass of meta content URL escaping causes XSS in html/template

[unknown] CVE-2026-39823 — pkg:golang/stdlib@1.25.9

Bypass of meta content URL escaping causes XSS in html/template

[unknown] CVE-2026-39823 — pkg:golang/stdlib@1.26.2

Bypass of meta content URL escaping causes XSS in html/template

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.29.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.30.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.33.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.42.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows

[unknown] CVE-2026-39825 — pkg:golang/stdlib@1.22.12

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] CVE-2026-39825 — pkg:golang/stdlib@1.23.6

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] CVE-2026-39825 — pkg:golang/stdlib@1.25.5

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] CVE-2026-39825 — pkg:golang/stdlib@1.25.9

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] CVE-2026-39825 — pkg:golang/stdlib@1.26.2

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] CVE-2026-39826 — pkg:golang/stdlib@1.22.12

Escaper bypass leads to XSS in html/template

[unknown] CVE-2026-39826 — pkg:golang/stdlib@1.23.6

Escaper bypass leads to XSS in html/template

[unknown] CVE-2026-39826 — pkg:golang/stdlib@1.25.5

Escaper bypass leads to XSS in html/template

[unknown] CVE-2026-39826 — pkg:golang/stdlib@1.25.9

Escaper bypass leads to XSS in html/template

[unknown] CVE-2026-39826 — pkg:golang/stdlib@1.26.2

Escaper bypass leads to XSS in html/template

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking memory leak when rejecting channels can lead to DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking bypass of certificate restrictions in golang.org/x/crypto/ssh

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking pathological RSA/DSA parameters may cause DoS in golang.org/x/crypto/ssh

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking client can cause server deadlock on unexpected responses in golang.org/x/crypto/ssh

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking bypass of FIDO/U2F security keys physical interaction in golang.org/x/crypto/ssh

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking agent constraints dropped when forwarding keys in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking key constraints not enforced in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking infinite loop on large channel writes in golang.org/x/crypto/ssh

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking server panic during CheckHostKey/Authenticate in golang.org/x/crypto/ssh

[unknown] CVE-2026-39836 — pkg:golang/stdlib@1.22.12

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] CVE-2026-39836 — pkg:golang/stdlib@1.23.6

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] CVE-2026-39836 — pkg:golang/stdlib@1.25.5

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] CVE-2026-39836 — pkg:golang/stdlib@1.25.9

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] CVE-2026-39836 — pkg:golang/stdlib@1.26.2

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] CVE-2026-39883 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

Opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking in go.opentelemetry.io/otel/sdk

[unknown] CVE-2026-39984 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has Improper Certificate Validation in verifier in github.com/sigstore/timestamp-authority

[unknown] CVE-2026-41178 — pkg:golang/go.opentelemetry.io/otel@v1.43.0

Opentelemetry-go's baggage parsing no longer caps raw header length in go.opentelemetry.io/otel

[unknown] CVE-2026-41506 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Go-git: Credential leak via cross-host redirect in smart HTTP transport in github.com/go-git/go-git

[unknown] CVE-2026-41506 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Go-git: Credential leak via cross-host redirect in smart HTTP transport in github.com/go-git/go-git

[unknown] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Docker: 'PUT /containers/{id}/archive' executes container binary on the host in github.com/docker/docker

[unknown] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Docker: 'PUT /containers/{id}/archive' executes container binary on the host in github.com/docker/docker

[unknown] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Docker: 'PUT /containers/{id}/archive' executes container binary on the host in github.com/docker/docker

[unknown] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Race condition in 'docker cp' in github.com/docker/docker allows creation of arbitrary files

[unknown] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Race condition in 'docker cp' in github.com/docker/docker allows creation of arbitrary files

[unknown] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Race condition in 'docker cp' in github.com/docker/docker allows creation of arbitrary files

[unknown] CVE-2026-41579 — pkg:golang/github.com/opencontainers/runc@v1.1.12

Malicious image with /dev symlink can trigger limited host filesystem integrity violations in github.com/opencontainers/runc

[unknown] CVE-2026-41888 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution's tag deletion bypasses `storage.delete.enabled` configuration in github.com/distribution/distribution

[unknown] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v25.0.6%2Bincompatible

Race condition in 'docker cp' in github.com/docker/docker allows bind mount redirection

[unknown] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v27.4.1%2Bincompatible

Race condition in 'docker cp' in github.com/docker/docker allows bind mount redirection

[unknown] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v28.0.0%2Bincompatible

Race condition in 'docker cp' in github.com/docker/docker allows bind mount redirection

[unknown] CVE-2026-42499 — pkg:golang/stdlib@1.22.12

Quadratic string concatenation in consumePhrase in net/mail

[unknown] CVE-2026-42499 — pkg:golang/stdlib@1.23.6

Quadratic string concatenation in consumePhrase in net/mail

[unknown] CVE-2026-42499 — pkg:golang/stdlib@1.25.5

Quadratic string concatenation in consumePhrase in net/mail

[unknown] CVE-2026-42499 — pkg:golang/stdlib@1.25.9

Quadratic string concatenation in consumePhrase in net/mail

[unknown] CVE-2026-42499 — pkg:golang/stdlib@1.26.2

Quadratic string concatenation in consumePhrase in net/mail

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.33.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.34.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.35.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.41.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.52.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42504 — pkg:golang/stdlib@1.22.12

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] CVE-2026-42504 — pkg:golang/stdlib@1.23.6

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] CVE-2026-42504 — pkg:golang/stdlib@1.25.5

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] CVE-2026-42504 — pkg:golang/stdlib@1.25.9

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] CVE-2026-42504 — pkg:golang/stdlib@1.26.2

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] CVE-2026-42505 — pkg:golang/stdlib@1.22.12

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] CVE-2026-42505 — pkg:golang/stdlib@1.23.6

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] CVE-2026-42505 — pkg:golang/stdlib@1.25.5

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] CVE-2026-42505 — pkg:golang/stdlib@1.25.9

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] CVE-2026-42505 — pkg:golang/stdlib@1.26.2

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.33.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.34.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.35.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.41.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.52.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

[unknown] CVE-2026-42507 — pkg:golang/stdlib@1.22.12

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] CVE-2026-42507 — pkg:golang/stdlib@1.23.6

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] CVE-2026-42507 — pkg:golang/stdlib@1.25.5

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] CVE-2026-42507 — pkg:golang/stdlib@1.25.9

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] CVE-2026-42507 — pkg:golang/stdlib@1.26.2

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking auth bypass via unenforced @revoked status in golang.org/x/crypto/ssh/knownhosts

[unknown] CVE-2026-44740 — pkg:golang/github.com/go-git/go-billy/v5@v5.5.0

Go-billy: Symlink resolution lack of cycle detection leads to infinite loop in github.com/go-git/go-billy

[unknown] CVE-2026-44740 — pkg:golang/github.com/go-git/go-billy/v5@v5.6.2

Go-billy: Symlink resolution lack of cycle detection leads to infinite loop in github.com/go-git/go-billy

[unknown] CVE-2026-44973 — pkg:golang/github.com/go-git/go-billy/v5@v5.5.0

Go-billy has path traversal vulnerabilities in github.com/go-git/go-billy

[unknown] CVE-2026-44973 — pkg:golang/github.com/go-git/go-billy/v5@v5.6.2

Go-billy has path traversal vulnerabilities in github.com/go-git/go-billy

[unknown] CVE-2026-45022 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Go-git: Improper parsing of specially crafted objects may lead to inconsistent interpretation in github.com/go-git/go-git

[unknown] CVE-2026-45022 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Go-git: Improper parsing of specially crafted objects may lead to inconsistent interpretation in github.com/go-git/go-git

[unknown] CVE-2026-45570 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Improper single-quote escaping in go-git SSH transport in github.com/go-git/go-git

[unknown] CVE-2026-45570 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Improper single-quote escaping in go-git SSH transport in github.com/go-git/go-git

[unknown] CVE-2026-45571 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Go-git: Crafted repositories may modify main and submodule .git directories in github.com/go-git/go-git

[unknown] CVE-2026-45571 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Go-git: Crafted repositories may modify main and submodule .git directories in github.com/go-git/go-git

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking VerifiedPublicKeyCallback permissions skip enforcement in golang.org/x/crypto/ssh

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking byte arithmetic causes underflow and panic in golang.org/x/crypto/ssh

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.32.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.33.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.39.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.49.0

Invoking pathological inputs can lead to client panic in golang.org/x/crypto/ssh/agent

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.33.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.34.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.35.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.41.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.52.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.55.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.55.0?type=module

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/stdlib@1.26.2

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-46600 — pkg:golang/stdlib@1.26.5

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

[unknown] CVE-2026-47262 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd image-triggered runtime DoS via unbounded group parsing in github.com/containerd/containerd

[unknown] CVE-2026-47262 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd image-triggered runtime DoS via unbounded group parsing in github.com/containerd/containerd

[unknown] CVE-2026-48702 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic in github.com/sigstore/rekor

[unknown] CVE-2026-48702 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic in github.com/sigstore/rekor

[unknown] CVE-2026-49478 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage in github.com/sigstore/fulcio

[unknown] CVE-2026-49478 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage in github.com/sigstore/fulcio

[unknown] CVE-2026-49834 — pkg:golang/github.com/sigstore/sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log in github.com/sigstore/sigstore-go

[unknown] CVE-2026-49835 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality in github.com/sigstore/timestamp-authority

[unknown] CVE-2026-50163 — pkg:golang/oras.land/oras-go/v2@v2.6.1

Hardlink path traversal during tar extraction in oras.land/oras-go

[unknown] CVE-2026-50195 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[unknown] CVE-2026-50195 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[unknown] CVE-2026-53488 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull in github.com/containerd/containerd

[unknown] CVE-2026-53488 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull in github.com/containerd/containerd

[unknown] CVE-2026-53489 — pkg:golang/github.com/containerd/containerd@v1.7.11

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[unknown] CVE-2026-53489 — pkg:golang/github.com/containerd/containerd@v1.7.32

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[unknown] CVE-2026-53492 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[unknown] CVE-2026-53492 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[unknown] CVE-2026-53495 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service in github.com/containerd/containerd

[unknown] CVE-2026-53495 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd: CRI ExecSync Goroutine Leak Leads to Node-Level Denial of Service in github.com/containerd/containerd

[unknown] CVE-2026-54167 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header in github.com/openshift-pipelines/pipelines-as-code

[unknown] CVE-2026-54167 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Pipelines-as-Code GitHub App token request can be redirected via untrusted Enterprise Host header in github.com/openshift-pipelines/pipelines-as-code

[unknown] CVE-2026-54168 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.31.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution in github.com/openshift-pipelines/pipelines-as-code

[unknown] CVE-2026-54168 — pkg:golang/github.com/openshift-pipelines/pipelines-as-code@v0.33.0

Tekton Pipelines-as-Code: Unscoped GitHub App installation token allows unauthorized access to private repositories via remote task resolution in github.com/openshift-pipelines/pipelines-as-code

[unknown] CVE-2026-54787 — pkg:golang/github.com/sigstore/sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period in github.com/sigstore/sigstore-go

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.21.0

Infinite loop on invalid input in golang.org/x/text

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.22.0

Infinite loop on invalid input in golang.org/x/text

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.26.0

Infinite loop on invalid input in golang.org/x/text

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.35.0

Infinite loop on invalid input in golang.org/x/text

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.37.0?type=module

Infinite loop on invalid input in golang.org/x/text

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.38.0

Infinite loop on invalid input in golang.org/x/text

[unknown] CVE-2026-56853 — pkg:golang/stdlib@1.22.12

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] CVE-2026-56853 — pkg:golang/stdlib@1.23.6

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] CVE-2026-56853 — pkg:golang/stdlib@1.25.5

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] CVE-2026-56853 — pkg:golang/stdlib@1.25.9

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] CVE-2026-56853 — pkg:golang/stdlib@1.26.2

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] CVE-2026-56853 — pkg:golang/stdlib@1.26.5

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] CVE-2026-56854 — pkg:golang/golang.org/x/crypto@v0.32.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] CVE-2026-56854 — pkg:golang/golang.org/x/crypto@v0.33.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] CVE-2026-56854 — pkg:golang/golang.org/x/crypto@v0.39.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] CVE-2026-56854 — pkg:golang/golang.org/x/crypto@v0.49.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] CVE-2026-56854 — pkg:golang/golang.org/x/crypto@v0.53.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] CVE-2026-56855 — pkg:golang/golang.org/x/crypto@v0.32.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-56855 — pkg:golang/golang.org/x/crypto@v0.33.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-56855 — pkg:golang/golang.org/x/crypto@v0.39.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-56855 — pkg:golang/golang.org/x/crypto@v0.49.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-56855 — pkg:golang/golang.org/x/crypto@v0.53.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-56858 — pkg:golang/stdlib@1.22.12

Fix Javascript regexp context tracking in html/template

[unknown] CVE-2026-56858 — pkg:golang/stdlib@1.23.6

Fix Javascript regexp context tracking in html/template

[unknown] CVE-2026-56858 — pkg:golang/stdlib@1.25.5

Fix Javascript regexp context tracking in html/template

[unknown] CVE-2026-56858 — pkg:golang/stdlib@1.25.9

Fix Javascript regexp context tracking in html/template

[unknown] CVE-2026-56858 — pkg:golang/stdlib@1.26.2

Fix Javascript regexp context tracking in html/template

[unknown] CVE-2026-56858 — pkg:golang/stdlib@1.26.5

Fix Javascript regexp context tracking in html/template

[unknown] CVE-2026-56859 — pkg:golang/stdlib@1.22.12

Add recursion depth guard during decode in encoding/xml

[unknown] CVE-2026-56859 — pkg:golang/stdlib@1.23.6

Add recursion depth guard during decode in encoding/xml

[unknown] CVE-2026-56859 — pkg:golang/stdlib@1.25.5

Add recursion depth guard during decode in encoding/xml

[unknown] CVE-2026-56859 — pkg:golang/stdlib@1.25.9

Add recursion depth guard during decode in encoding/xml

[unknown] CVE-2026-56859 — pkg:golang/stdlib@1.26.2

Add recursion depth guard during decode in encoding/xml

[unknown] CVE-2026-56859 — pkg:golang/stdlib@1.26.5

Add recursion depth guard during decode in encoding/xml

[unknown] CVE-2026-56860 — pkg:golang/stdlib@1.22.12

Avoid quadratic complexity in resolvePath in net/url

[unknown] CVE-2026-56860 — pkg:golang/stdlib@1.23.6

Avoid quadratic complexity in resolvePath in net/url

[unknown] CVE-2026-56860 — pkg:golang/stdlib@1.25.5

Avoid quadratic complexity in resolvePath in net/url

[unknown] CVE-2026-56860 — pkg:golang/stdlib@1.25.9

Avoid quadratic complexity in resolvePath in net/url

[unknown] CVE-2026-56860 — pkg:golang/stdlib@1.26.2

Avoid quadratic complexity in resolvePath in net/url

[unknown] CVE-2026-56860 — pkg:golang/stdlib@1.26.5

Avoid quadratic complexity in resolvePath in net/url

[unknown] CVE-2026-56862 — pkg:golang/stdlib@1.22.12

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] CVE-2026-56862 — pkg:golang/stdlib@1.23.6

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] CVE-2026-56862 — pkg:golang/stdlib@1.25.5

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] CVE-2026-56862 — pkg:golang/stdlib@1.25.9

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] CVE-2026-56862 — pkg:golang/stdlib@1.26.2

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] CVE-2026-56862 — pkg:golang/stdlib@1.26.5

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] CVE-2026-56864 — pkg:golang/golang.org/x/mod@v0.22.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] CVE-2026-56864 — pkg:golang/golang.org/x/mod@v0.25.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] CVE-2026-56864 — pkg:golang/golang.org/x/mod@v0.33.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] CVE-2026-56865 — pkg:golang/golang.org/x/mod@v0.22.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] CVE-2026-56865 — pkg:golang/golang.org/x/mod@v0.25.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] CVE-2026-56865 — pkg:golang/golang.org/x/mod@v0.33.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] CVE-2026-61711 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit: Custom frontend could bypass Seccomp/AppArmor in github.com/moby/buildkit

[unknown] CVE-2026-61711 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit: Custom frontend could bypass Seccomp/AppArmor in github.com/moby/buildkit

[unknown] CVE-2026-61712 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit has a possible runtime DoS via unbounded group parsing in github.com/moby/buildkit

[unknown] CVE-2026-61712 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit has a possible runtime DoS via unbounded group parsing in github.com/moby/buildkit

[unknown] CVE-2026-6383 — pkg:golang/kubevirt.io/kubevirt

KubeVirt's authorization mechanism improperly truncates subresource names in kubevirt.io/kubevirt

[unknown] CVE-2026-71556 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Worktree operations may follow symlinks in github.com/go-git/go-git

[unknown] CVE-2026-71556 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Worktree operations may follow symlinks in github.com/go-git/go-git

[unknown] CVE-2026-71557 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Path traversal via crafted reference names in github.com/go-git/go-git

[unknown] CVE-2026-71557 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Path traversal via crafted reference names in github.com/go-git/go-git

[unknown] CVE-2026-72816 — pkg:golang/github.com/go-chi/chi/v5@v5.1.0

Chi's RealIP Middleware allows IP spoofing via unvalidated X-Forwarded-For header in github.com/go-chi/chi

[unknown] CVE-2026-72817 — pkg:golang/github.com/go-chi/chi/v5@v5.1.0

Chi Middleware vulnerable to IP spoofing via X-Forwarded-For header in github.com/go-chi/chi

[unknown] CVE-2026-7374 — pkg:golang/kubevirt.io/kubevirt

KubeVirt has a Link Following vulnerability in kubevirt.io/kubevirt

[unknown] CVE-2026-78662 — pkg:golang/golang.org/x/crypto@v0.32.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-78662 — pkg:golang/golang.org/x/crypto@v0.33.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-78662 — pkg:golang/golang.org/x/crypto@v0.39.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-78662 — pkg:golang/golang.org/x/crypto@v0.49.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-78662 — pkg:golang/golang.org/x/crypto@v0.53.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.67.1

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.69.4

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.70.0

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.79.3

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] CVE-2026-84303 — pkg:golang/google.golang.org/grpc@v1.80.0

Bypass of xDS RBAC HTTP filter header matching in google.golang.org/grpc

[unknown] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.67.1

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.69.4

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.70.0

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.79.3

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] CVE-2026-84304 — pkg:golang/google.golang.org/grpc@v1.80.0

Heap Memory Exhaustion (OOM) via HTTP/2 DATA Frame Fragmentation in google.golang.org/grpc

[unknown] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.67.1

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.69.4

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.70.0

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.79.3

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] CVE-2026-84445 — pkg:golang/google.golang.org/grpc@v1.80.0

Server panic via missing authority or Host headers in google.golang.org/grpc

[unknown] CVE-2026-89090 — pkg:golang/github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream@v1.6.8

DoS due to Panic in AWS SDK for Go v2 SDK EventStream Decoder in github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream

[unknown] CVE-2026-89090 — pkg:golang/github.com/aws/aws-sdk-go-v2/service/s3@v1.76.0

DoS due to Panic in AWS SDK for Go v2 SDK EventStream Decoder in github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream

[unknown] CVE-2026-9804 — pkg:golang/kubevirt.io/kubevirt

KubeVirt has a Link Following issue in kubevirt.io/kubevirt

[unknown] GO-2022-1000 — pkg:golang/kubevirt.io/kubevirt

KubeVirt vulnerable to arbitrary file read on host in kubevirt.io/kubevirt

[unknown] GO-2026-4770 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

[unknown] GO-2026-5547 — pkg:golang/github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior in github.com/in-toto/in-toto-golang

[unknown] GO-2026-5693 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Go-git: Malformed Git object data may cause panics or resource exhaustion in github.com/go-git/go-git

[unknown] GO-2026-5693 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Go-git: Malformed Git object data may cause panics or resource exhaustion in github.com/go-git/go-git

[unknown] GO-2026-5841 — pkg:golang/github.com/klauspost/compress@v1.17.11

OOB read in github.com/klauspost/compress/s2

[unknown] GO-2026-5841 — pkg:golang/github.com/klauspost/compress@v1.17.7

OOB read in github.com/klauspost/compress/s2

[unknown] GO-2026-5841 — pkg:golang/github.com/klauspost/compress@v1.18.4

OOB read in github.com/klauspost/compress/s2

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.32.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.33.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.39.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.49.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.53.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.67.1

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.69.4

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.70.0

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.79.3

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.80.0

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

[unknown] GO-2026-6094 — pkg:golang/github.com/google/cel-go@v0.23.2

JSON private fields exposed via NativeTypes and ParseStructTag in github.com/google/cel-go

[unknown] GO-2026-6225 — pkg:golang/github.com/chrismellard/docker-credential-acr-env@v0.0.0-20230304212654-82a0ddb

Credential leakage to untrusted hosts in github.com/chrismellard/docker-credential-acr-env

[unknown] GO-2026-6278 — pkg:golang/github.com/gorilla/websocket@v1.5.0

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key in github.com/gorilla/websocket

[unknown] GO-2026-6278 — pkg:golang/github.com/gorilla/websocket@v1.5.0?type=module

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key in github.com/gorilla/websocket

[unknown] GO-2026-6278 — pkg:golang/github.com/gorilla/websocket@v1.5.0?type=package

Gorilla WebSocket Uses Cryptographically Weak PRNG for WebSocket Mask Key in github.com/gorilla/websocket

[unknown] RHBA-2017:1929 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Bug Fix Advisory: openssl bug fix and enhancement update

[unknown] RHBA-2017:1929 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Bug Fix Advisory: openssl bug fix and enhancement update

[unknown] RHBA-2022:3945 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Bug Fix Advisory: new packages: vim

[unknown] RHBA-2022:3945 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Bug Fix Advisory: new packages: vim

[unknown] RHBA-2022:3945 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Bug Fix Advisory: new packages: vim

[unknown] RHBA-2022:3945 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Bug Fix Advisory: new packages: vim

[unknown] RHBA-2025:12345 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Bug Fix Advisory: libxml2 and libxslt bug fix and enhancement update

[unknown] RHBA-2025:6314 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Bug Fix Advisory: openssl bug fix and enhancement update

[unknown] RHBA-2025:6314 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Bug Fix Advisory: openssl bug fix and enhancement update

[unknown] RHBA-2025:6597 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Bug Fix Advisory: libxml2 bug fix and enhancement update

[unknown] RHSA-2005:010 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:010 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:010 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:036 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:036 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:036 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:122 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:122 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:122 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:745 —

pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:745 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2005:745 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2007:0276 —
pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shadc

Red Hat Security Advisory: shadow-utils security and bug fix update

[unknown] RHSA-2007:0346 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2007:0346 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2007:0346 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2007:0431 —
pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shadc

Red Hat Security Advisory: shadow-utils security and bug fix update

[unknown] RHSA-2007:0860 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2008:0580 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0580 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0580 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0617 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0617 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0617 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0618 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0618 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2008:0618 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2010:0141 — pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2011:0558 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2011:0558 — pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2011:0558 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2011:0558 — pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2011:1424 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2011:1424 — pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl security update

[unknown] RHSA-2011:1424 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2011:1424 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2013:0685 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2013:0685 —
pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl security update

[unknown] RHSA-2013:0685 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2013:0685 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2014:0679 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2014:0679 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2014:1052 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2014:1052 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2014:1652 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2014:1652 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:0066 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:0066 —

pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:0716 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2015:0716 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2015:1072 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:1072 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:1115 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:1115 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:2617 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2015:2617 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0008 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0008 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0301 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0301 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0305 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0305 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0722 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:0722 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:1940 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:1940 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2016:2972 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2016:2972 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2016:2972 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2016:2972 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2017:0286 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2017:0286 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2018:0998 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2018:0998 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2018:3221 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2018:3221 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2019:0109 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:0109 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:0483 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2019:0483 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2019:1619 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1619 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1619 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1619 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1774 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1774 —

pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1774 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1774 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1790 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:1790 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:1793 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1793 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1793 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1793 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1942 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:1942 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:1947 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1947 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1947 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:1947 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2019:2304 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 9

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2019:2304 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2019:2400 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:2400 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2019:3700 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 9

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2019:3700 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2020:1840 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 9

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2020:1840 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2020:4453 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2020:4453 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2020:4453 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2020:4453 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2020:4514 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2020:4514 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2020:5422 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5422 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5476 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2020:5476 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2020:5566 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5566 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5588 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5588 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5623 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5623 —

pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5637 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5637 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5639 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5639 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5640 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5640 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5641 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5641 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5642 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2020:5642 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:0343 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:0343 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:0557 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:0557 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:0883 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:0883 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:1024 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:1024 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:1032 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:1032 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:1063 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:1063 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:1131 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:1131 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:1266 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:1266 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:1678 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2021:1678 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2021:2184 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:2184 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2021:2792 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2021:2792 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security and bug fix update

[unknown] RHSA-2021:3798 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:3798 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:4424 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2021:4424 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2021:4517 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2021:4517 —

pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2021:4517 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2021:4517 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2021:5226 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2021:5226 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:0064 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:0064 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:0366 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f4

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0366 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0366 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0366 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0894 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f4

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0894 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0894 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:0894 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:1065 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1065 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1066 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1066 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1071 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1071 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1076 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1076 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1077 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1077 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1078 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1078 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1082 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1082 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1091 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1091 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1112 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1112 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:1552 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:1552 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:1552 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:1552 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5242 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5242 —

pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5242 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5242 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5319 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5319 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5319 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5319 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5813 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5813 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5813 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5813 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5818 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:5818 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:5942 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5942 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5942 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:5942 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2022:6224 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2022:6224 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2022:7288 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2022:7288 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:0842 — pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2023:0946 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:0946 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:0958 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2023:0958 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2023:0958 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2023:0958 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2023:0959 — pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2023:1199 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:1199 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:1335 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1335 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1405 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1405 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1437 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1437 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1439 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1439 —

pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1440 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1440 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1441 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:1441 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:2523 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:2523 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:3408 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:3408 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:3722 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:3722 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security and bug fix update

[unknown] RHSA-2023:5610 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2023:6632 —
pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shado

Red Hat Security Advisory: shadow-utils security and bug fix update

[unknown] RHSA-2023:6661 — pkg:rpm/redhat/gmp@6.2.0-13.el9?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=gmp-6.2.0-1

Red Hat Security Advisory: gmp security and enhancement update

[unknown] RHSA-2023:7112 — pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shado

Red Hat Security Advisory: shadow-utils security and bug fix update

[unknown] RHSA-2023:7877 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2023:7877 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0154 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0154 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0208 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0208 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0310 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0310 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0417 — pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shado

Red Hat Security Advisory: shadow-utils security update

[unknown] RHSA-2024:0500 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:0500 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:1102 — pkg:rpm/redhat/gmp@6.2.0-13.el9?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=gmp-6.2.0-1

Red Hat Security Advisory: gmp security update

[unknown] RHSA-2024:1412 — pkg:rpm/redhat/gmp@6.2.0-13.el9?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=gmp-6.2.0-1

Red Hat Security Advisory: gmp update

[unknown] RHSA-2024:2228 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2024:2228 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2024:2447 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl and openssl-fips-provider security update

[unknown] RHSA-2024:2447 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl and openssl-fips-provider security update

[unknown] RHSA-2024:2577 — pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shado

Red Hat Security Advisory: shadow-utils security update

[unknown] RHSA-2024:3128 — pkg:rpm/redhat/perl-Digest@1.19-4.el9?arch=noarch&checksum=sha256%3Ae0b8633f818467f9e1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 — pkg:rpm/redhat/perl-Encode@3.08-462.el9?arch=x86_64&checksum=sha256%3Ad05248697e4892

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 — pkg:rpm/redhat/perl-File-Temp@0.231.100-4.el9?arch=noarch&checksum=sha256%3A0a81b0623 9

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 — pkg:rpm/redhat/perl-Getopt-Long@2.52-4.el9?arch=noarch&checksum=sha256%3A055fe33d2a7a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 — pkg:rpm/redhat/perl-HTTP-Tiny@0.076-462.el9?arch=noarch&checksum=sha256%3A696f388a50f

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —

pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-Pod-Usage@2.01-4.el9?arch=noarch&checksum=sha256%3Ac170870a2d1ff3

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-Scalar-List-Utils@1.56-462.el9?arch=x86_64&checksum=sha256%3A7ce874b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-Time-Local@1.300-7.el9?arch=noarch&checksum=sha256%3Ae8e1e692b6e5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-constant@1.33-461.el9?arch=noarch&checksum=sha256%3A8ab94e13cab4e7

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3128 —
pkg:rpm/redhat/perl-podlators@4.14-460.el9?arch=noarch&checksum=sha256%3A0401f715522a1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2024:3214 —
pkg:rpm/redhat/gmp@6.2.0-13.el9?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=gmp-6.2.0-1

Red Hat Security Advisory: gmp security update

[unknown] RHSA-2024:5136 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:5136 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:6783 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:6783 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:7846 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:7846 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:7847 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:7847 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:7848 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:7848 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2024:8906 — pkg:rpm/redhat/libsolv@0.7.24-6.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libsolv-0.7.24-6.e

Red Hat Security Advisory: Satellite 6.16.0 release

[unknown] RHSA-2024:9333 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl and openssl-fips-provider security update

[unknown] RHSA-2024:9333 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl and openssl-fips-provider security update

[unknown] RHSA-2024:9405 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2024:9405 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2024:9405 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2024:9405 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:10630 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2025:10768 — pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.18.20 packages and security update

[unknown] RHSA-2025:10855 — pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2025:11066 — pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2025:11066 — pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2025:11066 — pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2025:11545 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:11545 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:11804 —

pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:11804 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:11805 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:11805 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:11933 —
pkg:rpm/redhat/sqlite-libs@3.34.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=sqlite-3.34.1

Red Hat Security Advisory: sqlite security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-AutoLoader@5.74-481.1.el9_6?arch=noarch&checksum=sha256%3Ab4557d85

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-B@1.80-481.1.el9_6?arch=x86_64&checksum=sha256%3A8b5a3d27f69cce8d

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-Class-Struct@0.66-481.1.el9_6?arch=noarch&checksum=sha256%3Ad35ff343

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-DynaLoader@1.47-481.1.el9_6?arch=x86_64&checksum=sha256%3A937d31c

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-Errno@1.30-481.1.el9_6?arch=x86_64&checksum=sha256%3A9c03ad1166d9f

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-Fcntl@1.13-481.1.el9_6?arch=x86_64&checksum=sha256%3A72587bf21b268

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-File-Basename@2.85-481.1.el9_6?arch=noarch&checksum=sha256%3Ae39dc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 —
pkg:rpm/redhat/perl-File-stat@1.09-481.1.el9_6?arch=noarch&checksum=sha256%3Ab235134c19

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-FileHandle@2.03-481.1.el9_6?arch=noarch&checksum=sha256%3Ac2139abdb

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-Getopt-Std@1.12-481.1.el9_6?arch=noarch&checksum=sha256%3A49bd8381

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-IO@1.43-481.1.el9_6?arch=x86_64&checksum=sha256%3Ae29f5b38c643882

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-IPC-Open3@1.21-481.1.el9_6?arch=noarch&checksum=sha256%3A7ea36dcf2

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-NDBM_File@1.15-481.1.el9_6?arch=x86_64&checksum=sha256%3A1c340352

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-POSIX@1.94-481.1.el9_6?arch=x86_64&checksum=sha256%3A434ef22a697f3

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-SelectSaver@1.02-481.1.el9_6?arch=noarch&checksum=sha256%3A8ec404df

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-Symbol@1.08-481.1.el9_6?arch=noarch&checksum=sha256%3Aaa9942be4c8

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-base@2.27-481.1.el9_6?arch=noarch&checksum=sha256%3A0be44f0551078

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-if@0.60.800-481.1.el9_6?arch=noarch&checksum=sha256%3Aae3ce80bee55e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-lib@0.65-481.1.el9_6?arch=x86_64&checksum=sha256%3Abadc59793f32fa6e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-mro@1.23-481.1.el9_6?arch=x86_64&checksum=sha256%3A4ed671f36290bc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-overload@1.31-481.1.el9_6?arch=noarch&checksum=sha256%3Af172df7417

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-overloading@0.02-481.1.el9_6?arch=noarch&checksum=sha256%3A4aae487e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-subs@1.03-481.1.el9_6?arch=noarch&checksum=sha256%3A0a7ef4a9a174ab

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12056 — pkg:rpm/redhat/perl-vars@1.05-481.1.el9_6?arch=noarch&checksum=sha256%3A5d3c58094c0158

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:12882 — pkg:rpm/redhat/jq@1.6-19.el9_8.2?arch=x86_64&checksum=sha256%3A9793a39a4746a09ba89c3

Red Hat Security Advisory: jq security update

[unknown] RHSA-2025:13240 — pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2025:13240 — pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2025:13240 — pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2025:1330 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:1330 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:13429 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2025:14137 —

pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2025:17644 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17644 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17644 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17644 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17715 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17715 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17715 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17715 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17742 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17742 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17742 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17742 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17913 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17913 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17913 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:17913 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:19403 — pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: expat security update

[unknown] RHSA-2025:20126 — pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d09

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2025:20126 — pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2025:20145 — pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shado

Red Hat Security Advisory: shadow-utils security update

[unknown] RHSA-2025:20181 — pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: pam security update

[unknown] RHSA-2025:20559 — pkg:rpm/redhat/shadow-utils@4.9-16.el9?arch=x86_64&distro=rhel-9.8&epoch=2&upstream=shado

Red Hat Security Advisory: shadow-utils security update

[unknown] RHSA-2025:20945 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:20945 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:20945 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:20945 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:21015 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:21015 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:21015 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:21015 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:21030 — pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: expat security update

[unknown] RHSA-2025:21174 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21174 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21248 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21248 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21255 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21255 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21562 —

pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:21562 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:22019 —
pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: pam security update

[unknown] RHSA-2025:22794 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:22794 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:23479 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2025:23479 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2025:3666 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:3666 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2025:7440 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:7440 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:7440 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:7440 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-AutoLoader@5.74-481.1.el9_6?arch=noarch&checksum=sha256%3Ab4557d85

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-B@1.80-481.1.el9_6?arch=x86_64&checksum=sha256%3A8b5a3d27f69cce8d

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-Class-Struct@0.66-481.1.el9_6?arch=noarch&checksum=sha256%3Ad35ff343

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-DynaLoader@1.47-481.1.el9_6?arch=x86_64&checksum=sha256%3A937d31c

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-Errno@1.30-481.1.el9_6?arch=x86_64&checksum=sha256%3A9c03ad1166d9f

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-Fcntl@1.13-481.1.el9_6?arch=x86_64&checksum=sha256%3A72587bf21b268

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-File-Basename@2.85-481.1.el9_6?arch=noarch&checksum=sha256%3Ae39dc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-File-stat@1.09-481.1.el9_6?arch=noarch&checksum=sha256%3Ab235134c19

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-FileHandle@2.03-481.1.el9_6?arch=noarch&checksum=sha256%3Ac2139abdb

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-Getopt-Std@1.12-481.1.el9_6?arch=noarch&checksum=sha256%3A49bd8381

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-IO@1.43-481.1.el9_6?arch=x86_64&checksum=sha256%3Ae29f5b38c643882

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-IPC-Open3@1.21-481.1.el9_6?arch=noarch&checksum=sha256%3A7ea36dcf2

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-NDBM_File@1.15-481.1.el9_6?arch=x86_64&checksum=sha256%3A1c340352

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-POSIX@1.94-481.1.el9_6?arch=x86_64&checksum=sha256%3A434ef22a697f

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-SelectSaver@1.02-481.1.el9_6?arch=noarch&checksum=sha256%3A8ec404df

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-Symbol@1.08-481.1.el9_6?arch=noarch&checksum=sha256%3Aaa9942be4c8

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-base@2.27-481.1.el9_6?arch=noarch&checksum=sha256%3A0be44f0551078

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-if@0.60.800-481.1.el9_6?arch=noarch&checksum=sha256%3Aae3ce80bee55e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-lib@0.65-481.1.el9_6?arch=x86_64&checksum=sha256%3Abadc59793f32fa6e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-mro@1.23-481.1.el9_6?arch=x86_64&checksum=sha256%3A4ed671f36290bc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-overload@1.31-481.1.el9_6?arch=noarch&checksum=sha256%3Af172df7417

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-overloading@0.02-481.1.el9_6?arch=noarch&checksum=sha256%3A4aae487e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 — pkg:rpm/redhat/perl-subs@1.03-481.1.el9_6?arch=noarch&checksum=sha256%3A0a7ef4a9a174ab

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7500 —

pkg:rpm/redhat/perl-vars@1.05-481.1.el9_6?arch=noarch&checksum=sha256%3A5d3c58094c015

Red Hat Security Advisory: perl security update

[unknown] RHSA-2025:7510 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2025:7512 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: expat security update

[unknown] RHSA-2025:7517 —
pkg:rpm/redhat/sqlite-libs@3.34.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=sqlite-3.34.1-

Red Hat Security Advisory: sqlite security update

[unknown] RHSA-2025:7524 —
pkg:rpm/redhat/xz-libs@5.2.5-8.el9_0?arch=x86_64&distro=rhel-9.8&upstream=xz-5.2.5-8.el9_0.sr

Red Hat Security Advisory: xz security update

[unknown] RHSA-2025:9279 —
pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.19.1 packages and security update

[unknown] RHSA-2025:9418 —
pkg:rpm/redhat/krb5-libs@1.21.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=krb5-1.21.1-1

Red Hat Security Advisory: krb5 security update

[unknown] RHSA-2025:9420 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:0002 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2026:0067 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2026:0079 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:0079 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:0135 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2026:0337 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0337 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0434 — pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2026:0435 — pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security update

[unknown] RHSA-2026:0602 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0602 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0697 — pkg:rpm/redhat/gnupg2@2.3.3-5.el9_7?arch=x86_64&distro=rhel-9.8&upstream=gnupg2-2.3.3-5.el

Red Hat Security Advisory: gnupg2 security update

[unknown] RHSA-2026:0714 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0714 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0794 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl and openssl-fips-provider security update

[unknown] RHSA-2026:0794 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl and openssl-fips-provider security update

[unknown] RHSA-2026:0887 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0887 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:0975 — pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:10995 — pkg:rpm/redhat/sed@4.8-10.el9?arch=x86_64&distro=rhel-9.8&upstream=sed-4.8-10.el9.src.rpm

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:11004 — pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:11342 — pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:11389 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11389 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11389 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11389 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11503 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:11509 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11509 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11509 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11509 —

pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11510 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11510 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11510 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:11510 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:12423 —
pkg:rpm/redhat/libcap@2.48-10.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=libcap-2.48-10.el

Red Hat Security Advisory: libcap security update

[unknown] RHSA-2026:12740 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:1327 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:13274 —
pkg:rpm/redhat/gnutls@3.8.10-8.el9_8?arch=x86_64&distro=rhel-9.8&upstream=gnutls-3.8.10-8.el

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:1334 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:1334 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:1334 —
pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:13380 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d09

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:13380 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:1349 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1349 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:13651 —
pkg:rpm/redhat/systemd-libs@252-67.el9_8.4?arch=x86_64&distro=rhel-9.8&upstream=systemd-2

Red Hat Security Advisory: systemd security update

[unknown] RHSA-2026:14217 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:1472 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1472 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1473 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1473 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1475 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1475 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1477 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:1496 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1496 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1503 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1503 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1519 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1519 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1594 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1594 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:15969 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:1629 —
pkg:rpm/redhat/gnupg2@2.3.3-5.el9_7?arch=x86_64&distro=rhel-9.8&upstream=gnupg2-2.3.3-5.el

Red Hat Security Advisory: gnupg2 security update

[unknown] RHSA-2026:16692 —
pkg:rpm/redhat/jq@1.6-19.el9_8.2?arch=x86_64&checksum=sha256%3A9793a39a4746a09ba89c3

Red Hat Security Advisory: jq security update

[unknown] RHSA-2026:1696 —
pkg:rpm/redhat/libblkid@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.37.4-2

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1696 —
pkg:rpm/redhat/libfdisk@2.37.4-25.el9?arch=x86_64&checksum=sha256%3A1b861f267752e718ce

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1696 —

pkg:rpm/redhat/libmount@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.37.4

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1696 — pkg:rpm/redhat/libsmartcols@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.3

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1696 — pkg:rpm/redhat/libuuid@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.37.4-2

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1696 — pkg:rpm/redhat/util-linux@2.37.4-25.el9?arch=x86_64&checksum=sha256%3A35e0b73e574a7d8e

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1696 — pkg:rpm/redhat/util-linux-core@2.37.4-25.el9?arch=x86_64&checksum=sha256%3A5575c8fc753d

Red Hat Security Advisory: util-linux security update

[unknown] RHSA-2026:1720 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1720 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1733 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:1733 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:18040 — pkg:rpm/redhat/jq@1.6-19.el9_8.2?arch=x86_64&checksum=sha256%3A9793a39a4746a09ba89c3

Red Hat Security Advisory: jq security update

[unknown] RHSA-2026:18139 — pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:18139 — pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:18139 — pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:18153 —
pkg:rpm/redhat/systemd-libs@252-67.el9_8.4?arch=x86_64&distro=rhel-9.8&upstream=systemd-2

Red Hat Security Advisory: systemd security update

[unknown] RHSA-2026:1825 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:19061 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:19061 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:19061 —
pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:19066 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:19066 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:19068 —
pkg:rpm/redhat/systemd-libs@252-67.el9_8.4?arch=x86_64&distro=rhel-9.8&upstream=systemd-2

Red Hat Security Advisory: systemd security update

[unknown] RHSA-2026:19069 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:19069 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:19073 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:19073 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:19130 —
pkg:rpm/redhat/libcap@2.48-10.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=libcap-2.48-10.el

Red Hat Security Advisory: libcap security update

[unknown] RHSA-2026:19145 —
pkg:rpm/redhat/krb5-libs@1.21.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=krb5-1.21.1-1

Red Hat Security Advisory: krb5 security update

[unknown] RHSA-2026:19148 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:19151 —
pkg:rpm/redhat/jq@1.6-19.el9_8.2?arch=x86_64&checksum=sha256%3A9793a39a4746a09ba89c3

Red Hat Security Advisory: jq security update

[unknown] RHSA-2026:19218 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:19218 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:19224 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:19224 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:19456 —
pkg:rpm/redhat/libcap@2.48-10.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=libcap-2.48-10.el

Red Hat Security Advisory: libcap security update

[unknown] RHSA-2026:19567 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:20594 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:20594 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:20594 —
pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:21333 —

pkg:rpm/redhat/libsolv@0.7.24-6.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libsolv-0.7.24-6.e

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:21701 —
pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.20.24 packages and security update

[unknown] RHSA-2026:22312 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:22312 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:22314 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:22314 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:22711 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:22715 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: expat security update

[unknown] RHSA-2026:22717 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:22730 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:25237 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:25237 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:25239 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:25239 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:25900 —
pkg:rpm/redhat/systemd-libs@252-67.el9_8.4?arch=x86_64&distro=rhel-9.8&upstream=systemd-2

Red Hat Security Advisory: systemd security update

[unknown] RHSA-2026:26275 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:26275 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:26357 —
pkg:rpm/redhat/ncurses@6.2-12.20210508.el9?arch=x86_64&checksum=sha256%3Ad2835ed9dbf

Red Hat Security Advisory: ncurses security update

[unknown] RHSA-2026:26357 —
pkg:rpm/redhat/ncurses-base@6.2-12.20210508.el9?arch=noarch&distro=rhel-9.8&upstream=ncur

Red Hat Security Advisory: ncurses security update

[unknown] RHSA-2026:26357 —
pkg:rpm/redhat/ncurses-libs@6.2-12.20210508.el9?arch=x86_64&distro=rhel-9.8&upstream=ncurs

Red Hat Security Advisory: ncurses security update

[unknown] RHSA-2026:26573 —
pkg:rpm/redhat/libblkid@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.37.4-2

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:26573 —
pkg:rpm/redhat/util-linux@2.37.4-25.el9?arch=x86_64&checksum=sha256%3A35e0b73e574a7d8e

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:2719 —
pkg:rpm/redhat/gnupg2@2.3.3-5.el9_7?arch=x86_64&distro=rhel-9.8&upstream=gnupg2-2.3.3-5.el

Red Hat Security Advisory: gnupg2 security update

[unknown] RHSA-2026:2753 —
pkg:rpm/redhat/gnupg2@2.3.3-5.el9_7?arch=x86_64&distro=rhel-9.8&upstream=gnupg2-2.3.3-5.el

Red Hat Security Advisory: gnupg2 security update

[unknown] RHSA-2026:27745 —
pkg:rpm/redhat/openssl-fips-provider@3.0.7-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=op

Red Hat Security Advisory: openssl-fips-provider security update

[unknown] RHSA-2026:27745 —
pkg:rpm/redhat/openssl-fips-provider-so@3.0.7-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: openssl-fips-provider security update

[unknown] RHSA-2026:27746 —
pkg:rpm/redhat/openssl-fips-provider@3.0.7-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=op

Red Hat Security Advisory: openssl-fips-provider security update

[unknown] RHSA-2026:27746 —
pkg:rpm/redhat/openssl-fips-provider-so@3.0.7-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: openssl-fips-provider security update

[unknown] RHSA-2026:28049 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28049 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28049 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28049 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28050 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28050 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28050 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28050 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28133 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28133 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28133 —

pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28133 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28209 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28209 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28210 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28210 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28234 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:28235 —
pkg:rpm/redhat/libtasn1@4.16.0-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libtasn1-4.16.0

Red Hat Security Advisory: libtasn1 security update

[unknown] RHSA-2026:28236 —
pkg:rpm/redhat/libsolv@0.7.24-6.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libsolv-0.7.24-6.e

Red Hat Security Advisory: libsolv security update

[unknown] RHSA-2026:28491 —
pkg:rpm/redhat/rpm@4.16.1.3-40.el9?arch=x86_64&distro=rhel-9.8&upstream=rpm-4.16.1.3-40.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:28553 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:28553 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:29986 —
pkg:rpm/redhat/jq@1.6-19.el9_8.2?arch=x86_64&checksum=sha256%3A9793a39a4746a09ba89c3

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:30333 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:3042 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:3042 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:30647 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:30649 —
pkg:rpm/redhat/libsolv@0.7.24-6.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libsolv-0.7.24-6.e

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-Digest@1.19-4.el9?arch=noarch&checksum=sha256%3Ae0b8633f818467f9e1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-Encode@3.08-462.el9?arch=x86_64&checksum=sha256%3Ad05248697e4892

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-File-Temp@0.231.100-4.el9?arch=noarch&checksum=sha256%3A0a81b0623

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-Getopt-Long@2.52-4.el9?arch=noarch&checksum=sha256%3A055fe33d2a7a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-HTTP-Tiny@0.076-462.el9?arch=noarch&checksum=sha256%3A696f388a50f

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 —
pkg:rpm/redhat/perl-Pod-Usage@2.01-4.el9?arch=noarch&checksum=sha256%3Ac170870a2d1ff3

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-Scalar-List-Utils@1.56-462.el9?arch=x86_64&checksum=sha256%3A7ce874b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-Time-Local@1.300-7.el9?arch=noarch&checksum=sha256%3Ae8e1e692b6e5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-constant@1.33-461.el9?arch=noarch&checksum=sha256%3A8ab94e13cab4e7

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30851 — pkg:rpm/redhat/perl-podlators@4.14-460.el9?arch=noarch&checksum=sha256%3A0401f715522a1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:30900 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:30900 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:30900 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:30900 —

pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:33092 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security, bug fix, and enhancement update

[unknown] RHSA-2026:33092 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: glibc security, bug fix, and enhancement update

[unknown] RHSA-2026:33092 —
pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security, bug fix, and enhancement update

[unknown] RHSA-2026:33124 —
pkg:rpm/redhat/coreutils-single@8.32-41.el9_8?arch=x86_64&distro=rhel-9.8&upstream=coreutils-

Red Hat Security Advisory: coreutils security update

[unknown] RHSA-2026:33170 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:33170 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:33170 —
pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:33453 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:33453 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:33453 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:33453 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:33507 —
pkg:rpm/redhat/rpm@4.16.1.3-40.el9?arch=x86_64&distro=rhel-9.8&upstream=rpm-4.16.1.3-40.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:33635 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:3364 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:3364 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:33771 —
pkg:rpm/redhat/gzip@1.12-1.el9?arch=x86_64&checksum=sha256%3Ac8b3e0414d55b1eedb0185

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:33840 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:3437 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:3437 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:34476 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f4

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34476 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34476 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34476 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34477 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f4

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34477 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34477 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:34477 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:35016 —
pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:35454 —
pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.4

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:36759 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Digest@1.19-4.el9?arch=noarch&checksum=sha256%3Ae0b8633f818467f9e1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Encode@3.08-462.el9?arch=x86_64&checksum=sha256%3Ad05248697e4892

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-File-Temp@0.231.100-4.el9?arch=noarch&checksum=sha256%3A0a81b0623

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Getopt-Long@2.52-4.el9?arch=noarch&checksum=sha256%3A055fe33d2a7a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-HTTP-Tiny@0.076-462.el9?arch=noarch&checksum=sha256%3A696f388a50f

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —

pkg:rpm/redhat/perl-Pod-Usage@2.01-4.el9?arch=noarch&checksum=sha256%3Ac170870a2d1ff3

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Scalar-List-Utils@1.56-462.el9?arch=x86_64&checksum=sha256%3A7ce874b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-Time-Local@1.300-7.el9?arch=noarch&checksum=sha256%3Ae8e1e692b6e5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-constant@1.33-461.el9?arch=noarch&checksum=sha256%3A8ab94e13cab4e7

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5c

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37070 —
pkg:rpm/redhat/perl-podlators@4.14-460.el9?arch=noarch&checksum=sha256%3A0401f715522a1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:37382 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d09

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:37764 —
pkg:rpm/redhat/gzip@1.12-1.el9?arch=x86_64&checksum=sha256%3Ac8b3e0414d55b1eedb0185a

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:38279 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:38342 —
pkg:rpm/redhat/p11-kit@0.26.4-1.el9_8?arch=x86_64&distro=rhel-9.8&upstream=p11-kit-0.26.4-1.

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:38503 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:38503 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:38509 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:38510 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:38511 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:38804 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:38804 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:38805 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:38805 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:39304 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:39985 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:40041 —
pkg:rpm/redhat/gawk@5.1.0-6.el9?arch=x86_64&distro=rhel-9.8&upstream=gawk-5.1.0-6.el9.src.r

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:40485 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:40486 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:41176 —
pkg:rpm/redhat/libevent@2.1.12-8.el9_4?arch=x86_64&distro=rhel-9.8&upstream=libevent-2.1.12-

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:4163 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:4163 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:42063 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:42125 —
pkg:rpm/redhat/libidn2@2.3.0-7.el9?arch=x86_64&distro=rhel-9.8&upstream=libidn2-2.3.0-7.el9.sr

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:4214 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:4214 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:42329 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:42694 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:42694 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:42694 —

pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: glibc security update

[unknown] RHSA-2026:42739 —
pkg:rpm/redhat/libacl@2.4.0-1.el9_8?arch=x86_64&distro=rhel-9.8&upstream=acl-2.4.0-1.el9_8.sr

Red Hat Security Advisory: acl security update

[unknown] RHSA-2026:43513 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:43513 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:43818 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:4442 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:4442 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:4715 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:4715 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:47757 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:47757 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:47982 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f4

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:47982 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Digest@1.19-4.el9?arch=noarch&checksum=sha256%3Ae0b8633f818467f9e1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Encode@3.08-462.el9?arch=x86_64&checksum=sha256%3Ad05248697e4892

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-File-Temp@0.231.100-4.el9?arch=noarch&checksum=sha256%3A0a81b0623

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Getopt-Long@2.52-4.el9?arch=noarch&checksum=sha256%3A055fe33d2a7a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-HTTP-Tiny@0.076-462.el9?arch=noarch&checksum=sha256%3A696f388a50f

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Pod-Usage@2.01-4.el9?arch=noarch&checksum=sha256%3Ac170870a2d1ff3

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Scalar-List-Utils@1.56-462.el9?arch=x86_64&checksum=sha256%3A7ce874b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-Time-Local@1.300-7.el9?arch=noarch&checksum=sha256%3Ae8e1e692b6e5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 — pkg:rpm/redhat/perl-constant@1.33-461.el9?arch=noarch&checksum=sha256%3A8ab94e13cab4e7

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48225 —
pkg:rpm/redhat/perl-podlators@4.14-460.el9?arch=noarch&checksum=sha256%3A0401f715522a1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:48650 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:48650 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:48703 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:48703 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:48818 —
pkg:rpm/redhat/libsolv@0.7.24-6.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libsolv-0.7.24-6.e

Red Hat Security Advisory: libsolv security update

[unknown] RHSA-2026:49361 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:49661 —
pkg:rpm/redhat/gawk@5.1.0-6.el9?arch=x86_64&distro=rhel-9.8&upstream=gawk-5.1.0-6.el9.src.r

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:49668 —
pkg:rpm/redhat/p11-kit@0.26.4-1.el9_8?arch=x86_64&distro=rhel-9.8&upstream=p11-kit-0.26.4-1.

Red Hat Security Advisory: p11-kit security update

[unknown] RHSA-2026:49668 —

pkg:rpm/redhat/p11-kit-trust@0.26.4-1.el9_8?arch=x86_64&distro=rhel-9.8&upstream=p11-kit-0.2

Red Hat Security Advisory: p11-kit security update

[unknown] RHSA-2026:50144 —
pkg:rpm/redhat/libgcrypt@1.10.0-13.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libgcrypt-1.10

Red Hat Security Advisory: libgcrypt security update

[unknown] RHSA-2026:50223 —
pkg:rpm/redhat/libsolv@0.7.24-6.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libsolv-0.7.24-6.e

Red Hat Security Advisory: Satellite 6.16.12 Async Update

[unknown] RHSA-2026:50262 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:50262 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:5063 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:50807 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:51185 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:52414 —
pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.43

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:52675 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:52951 —
pkg:rpm/redhat/libgcrypt@1.10.0-13.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libgcrypt-1.10

Red Hat Security Advisory: libgcrypt security update

[unknown] RHSA-2026:53069 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:5396 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPM Release

[unknown] RHSA-2026:54552 —
pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.19.43 packages and security update

[unknown] RHSA-2026:54580 —
pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.20.34 packages and security update

[unknown] RHSA-2026:54650 —
pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.4

Red Hat Security Advisory: nghttp2 security update

[unknown] RHSA-2026:54662 —
pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.4

Red Hat Security Advisory: nghttp2 security update

[unknown] RHSA-2026:5475 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: Red Hat Hardened Images RPM Release

[unknown] RHSA-2026:54869 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:55431 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:55431 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:55432 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:55439 —
pkg:rpm/redhat/curl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.1-4

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:55439 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:55440 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:55450 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:5602 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:5602 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:56097 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:56133 — pkg:rpm/redhat/libattr@2.5.1-3.el9?arch=x86_64&distro=rhel-9.8&upstream=attr-2.5.1-3.el9.src.rp

Red Hat Security Advisory: attr security update

[unknown] RHSA-2026:56954 — pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:56984 — pkg:rpm/redhat/popt@1.18-8.el9?arch=x86_64&distro=rhel-9.8&upstream=popt-1.18-8.el9.src.rpm

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:57015 — pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:57361 — pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.22.11 packages and security update

[unknown] RHSA-2026:57482 — pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.18.54 packages and security update

[unknown] RHSA-2026:57604 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:57614 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f4

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:57614 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:57614 —

pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:57614 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:58503 —
pkg:rpm/redhat/libgcc@11.5.0-14.el9?arch=x86_64&distro=rhel-9.8&upstream=gcc-11.5.0-14.el9.s

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:58503 —
pkg:rpm/redhat/libstdc%2B%2B@11.5.0-14.el9?arch=x86_64&distro=rhel-9.8&upstream=gcc-11.5.

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:58563 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:58563 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:58927 —
pkg:rpm/redhat/sqlite-libs@3.34.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=sqlite-3.34.1

Red Hat Security Advisory: sqlite security update

[unknown] RHSA-2026:58936 —
pkg:rpm/redhat/sqlite-libs@3.34.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=sqlite-3.34.1

Red Hat Security Advisory: sqlite security update

[unknown] RHSA-2026:5913 —
pkg:rpm/redhat/ncurses@6.2-12.20210508.el9?arch=x86_64&checksum=sha256%3Ad2835ed9dbf

Red Hat Security Advisory: ncurses security update

[unknown] RHSA-2026:5913 —
pkg:rpm/redhat/ncurses-base@6.2-12.20210508.el9?arch=noarch&distro=rhel-9.8&upstream=ncur

Red Hat Security Advisory: ncurses security update

[unknown] RHSA-2026:5913 —
pkg:rpm/redhat/ncurses-libs@6.2-12.20210508.el9?arch=x86_64&distro=rhel-9.8&upstream=ncurs

Red Hat Security Advisory: ncurses security update

[unknown] RHSA-2026:59379 —
pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: pam security update

[unknown] RHSA-2026:59380 —
pkg:rpm/redhat/libattr@2.5.1-3.el9?arch=x86_64&distro=rhel-9.8&upstream=attr-2.5.1-3.el9.src.rp

Red Hat Security Advisory: attr security update

[unknown] RHSA-2026:59641 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:59641 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:59721 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:60018 —
pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.17.57 packages and security update

[unknown] RHSA-2026:60226 —
pkg:rpm/redhat/libattr@2.5.1-3.el9?arch=x86_64&distro=rhel-9.8&upstream=attr-2.5.1-3.el9.src.rp

Red Hat Security Advisory: attr security update

[unknown] RHSA-2026:60394 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:60451 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:60853 —
pkg:rpm/redhat/libevent@2.1.12-8.el9_4?arch=x86_64&distro=rhel-9.8&upstream=libevent-2.1.12-

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:60865 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:61229 —
pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: pam security update

[unknown] RHSA-2026:61247 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:61581 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security, bug fix, and enhancement update

[unknown] RHSA-2026:61586 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security, bug fix, and enhancement update

[unknown] RHSA-2026:61623 — pkg:rpm/redhat/gzip@1.12-1.el9?arch=x86_64&checksum=sha256%3Ac8b3e0414d55b1eedb0185a

Red Hat Security Advisory: gzip security update

[unknown] RHSA-2026:61625 — pkg:rpm/redhat/gzip@1.12-1.el9?arch=x86_64&checksum=sha256%3Ac8b3e0414d55b1eedb0185a

Red Hat Security Advisory: gzip security update

[unknown] RHSA-2026:61697 — pkg:rpm/redhat/sqlite-libs@3.34.1-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=sqlite-3.34.1-

Red Hat Security Advisory: sqlite security update

[unknown] RHSA-2026:61737 — pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:6190 — pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.43

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:63161 — pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.1

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:63162 — pkg:rpm/redhat/libblkid@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.37.4-2

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:63162 — pkg:rpm/redhat/util-linux@2.37.4-25.el9?arch=x86_64&checksum=sha256%3A35e0b73e574a7d8e

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:63388 — pkg:rpm/redhat/libevent@2.1.12-8.el9_4?arch=x86_64&distro=rhel-9.8&upstream=libevent-2.1.12-

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:64463 — pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:6463 — pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d09

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:6463 — pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:64787 —

pkg:rpm/redhat/xz-libs@5.2.5-8.el9_0?arch=x86_64&distro=rhel-9.8&upstream=xz-5.2.5-8.el9_0.sr

Red Hat Security Advisory: xz security update

[unknown] RHSA-2026:64799 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:64800 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:64810 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: expat security update

[unknown] RHSA-2026:64812 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: expat security update

[unknown] RHSA-2026:64815 —
pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: pam security update

[unknown] RHSA-2026:6502 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6502 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6502 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6502 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:65339 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:6539 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6539 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6539 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6539 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6540 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6540 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6540 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6540 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:65568 — pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:65767 — pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:6617 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6617 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6617 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6617 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6619 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6619 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6619 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6619 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6620 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6620 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6620 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6620 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66336 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66336 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66348 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66348 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66350 — pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.21.33 packages and security update

[unknown] RHSA-2026:66366 —

pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66366 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:66403 —
pkg:rpm/redhat/coreutils-single@8.32-41.el9_8?arch=x86_64&distro=rhel-9.8&upstream=coreutils-

Red Hat Security Advisory: coreutils security update

[unknown] RHSA-2026:66514 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:67154 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411 93

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2026:67154 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-AutoLoader@5.74-481.1.el9_6?arch=noarch&checksum=sha256%3Ab4557d85

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-B@1.80-481.1.el9_6?arch=x86_64&checksum=sha256%3A8b5a3d27f69cce8d

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-Class-Struct@0.66-481.1.el9_6?arch=noarch&checksum=sha256%3Ad35ff343

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-DynaLoader@1.47-481.1.el9_6?arch=x86_64&checksum=sha256%3A937d31c

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-Errno@1.30-481.1.el9_6?arch=x86_64&checksum=sha256%3A9c03ad1166d9f

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-Fcntl@1.13-481.1.el9_6?arch=x86_64&checksum=sha256%3A72587bf21b268

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 —
pkg:rpm/redhat/perl-File-Basename@2.85-481.1.el9_6?arch=noarch&checksum=sha256%3Ae39dc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-File-stat@1.09-481.1.el9_6?arch=noarch&checksum=sha256%3Ab235134c19

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-FileHandle@2.03-481.1.el9_6?arch=noarch&checksum=sha256%3Ac2139abdb

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-Getopt-Std@1.12-481.1.el9_6?arch=noarch&checksum=sha256%3A49bd8381

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-IO@1.43-481.1.el9_6?arch=x86_64&checksum=sha256%3Ae29f5b38c643882

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-IPC-Open3@1.21-481.1.el9_6?arch=noarch&checksum=sha256%3A7ea36dcf2

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-NDBM_File@1.15-481.1.el9_6?arch=x86_64&checksum=sha256%3A1c340352

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-POSIX@1.94-481.1.el9_6?arch=x86_64&checksum=sha256%3A434ef22a697f3

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-SelectSaver@1.02-481.1.el9_6?arch=noarch&checksum=sha256%3A8ec404df

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-Symbol@1.08-481.1.el9_6?arch=noarch&checksum=sha256%3Aaa9942be4c8

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-base@2.27-481.1.el9_6?arch=noarch&checksum=sha256%3A0be44f0551078

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-if@0.60.800-481.1.el9_6?arch=noarch&checksum=sha256%3Aae3ce80bee55e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-lib@0.65-481.1.el9_6?arch=x86_64&checksum=sha256%3Abadc59793f32fa6e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-mro@1.23-481.1.el9_6?arch=x86_64&checksum=sha256%3A4ed671f36290bc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-overload@1.31-481.1.el9_6?arch=noarch&checksum=sha256%3Af172df7417

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-overloading@0.02-481.1.el9_6?arch=noarch&checksum=sha256%3A4aae487e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-subs@1.03-481.1.el9_6?arch=noarch&checksum=sha256%3A0a7ef4a9a174ab

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67155 — pkg:rpm/redhat/perl-vars@1.05-481.1.el9_6?arch=noarch&checksum=sha256%3A5d3c58094c0158

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-AutoLoader@5.74-481.1.el9_6?arch=noarch&checksum=sha256%3Ab4557d85

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-B@1.80-481.1.el9_6?arch=x86_64&checksum=sha256%3A8b5a3d27f69cce8d

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-Class-Struct@0.66-481.1.el9_6?arch=noarch&checksum=sha256%3Ad35ff343

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-DynaLoader@1.47-481.1.el9_6?arch=x86_64&checksum=sha256%3A937d31c

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-Errno@1.30-481.1.el9_6?arch=x86_64&checksum=sha256%3A9c03ad1166d9f

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-Fcntl@1.13-481.1.el9_6?arch=x86_64&checksum=sha256%3A72587bf21b268

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —

pkg:rpm/redhat/perl-File-Basename@2.85-481.1.el9_6?arch=noarch&checksum=sha256%3Ae39dc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-File-stat@1.09-481.1.el9_6?arch=noarch&checksum=sha256%3Ab235134c19

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-FileHandle@2.03-481.1.el9_6?arch=noarch&checksum=sha256%3Ac2139abdb

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-Getopt-Std@1.12-481.1.el9_6?arch=noarch&checksum=sha256%3A49bd8381

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-IO@1.43-481.1.el9_6?arch=x86_64&checksum=sha256%3Ae29f5b38c643882

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-IPC-Open3@1.21-481.1.el9_6?arch=noarch&checksum=sha256%3A7ea36dcf2

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-NDBM_File@1.15-481.1.el9_6?arch=x86_64&checksum=sha256%3A1c340352

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-POSIX@1.94-481.1.el9_6?arch=x86_64&checksum=sha256%3A434ef22a697f3

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-SelectSaver@1.02-481.1.el9_6?arch=noarch&checksum=sha256%3A8ec404df

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-Symbol@1.08-481.1.el9_6?arch=noarch&checksum=sha256%3Aaa9942be4c8

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-base@2.27-481.1.el9_6?arch=noarch&checksum=sha256%3A0be44f0551078

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-if@0.60.800-481.1.el9_6?arch=noarch&checksum=sha256%3Aae3ce80bee55e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-lib@0.65-481.1.el9_6?arch=x86_64&checksum=sha256%3Abadc59793f32fa6e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-mro@1.23-481.1.el9_6?arch=x86_64&checksum=sha256%3A4ed671f36290bc

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-overload@1.31-481.1.el9_6?arch=noarch&checksum=sha256%3Af172df7417

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-overloading@0.02-481.1.el9_6?arch=noarch&checksum=sha256%3A4aae487e

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-subs@1.03-481.1.el9_6?arch=noarch&checksum=sha256%3A0a7ef4a9a174ab

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67156 — pkg:rpm/redhat/perl-vars@1.05-481.1.el9_6?arch=noarch&checksum=sha256%3A5d3c58094c0158

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67162 — pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67162 — pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl security update

[unknown] RHSA-2026:67165 — pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2026:67165 — pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security, bug fix, and enhancement update

[unknown] RHSA-2026:6725 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6725 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6725 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6725 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Digest@1.19-4.el9?arch=noarch&checksum=sha256%3Ae0b8633f818467f9e1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Encode@3.08-462.el9?arch=x86_64&checksum=sha256%3Ad05248697e4892

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-File-Temp@0.231.100-4.el9?arch=noarch&checksum=sha256%3A0a81b0623

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Getopt-Long@2.52-4.el9?arch=noarch&checksum=sha256%3A055fe33d2a7a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-HTTP-Tiny@0.076-462.el9?arch=noarch&checksum=sha256%3A696f388a50f

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Pod-Usage@2.01-4.el9?arch=noarch&checksum=sha256%3Ac170870a2d1ff3

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Scalar-List-Utils@1.56-462.el9?arch=x86_64&checksum=sha256%3A7ce874b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 — pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —

pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —
pkg:rpm/redhat/perl-Time-Local@1.300-7.el9?arch=noarch&checksum=sha256%3Ae8e1e692b6e5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —
pkg:rpm/redhat/perl-constant@1.33-461.el9?arch=noarch&checksum=sha256%3A8ab94e13cab4e

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:67278 —
pkg:rpm/redhat/perl-podlators@4.14-460.el9?arch=noarch&checksum=sha256%3A0401f715522a1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:6729 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6729 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6729 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6729 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6730 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6730 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6730 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6730 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6731 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6731 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6731 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6731 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6736 — pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6736 — pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6736 — pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6736 — pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:67534 — pkg:rpm/redhat/pcre2@10.40-6.el9?arch=x86_64&distro=rhel-9.8&upstream=pcre2-10.40-6.el9.src

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:67534 — pkg:rpm/redhat/pcre2-syntax@10.40-6.el9?arch=noarch&distro=rhel-9.8&upstream=pcre2-10.40-6

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:67886 — pkg:rpm/redhat/coreutils-single@8.32-41.el9_8?arch=x86_64&distro=rhel-9.8&upstream=coreutils-

Red Hat Security Advisory: coreutils security update

[unknown] RHSA-2026:67909 —
pkg:rpm/redhat/libevent@2.1.12-8.el9_4?arch=x86_64&distro=rhel-9.8&upstream=libevent-2.1.12-

Red Hat Security Advisory: libevent security update

[unknown] RHSA-2026:67910 —
pkg:rpm/redhat/libevent@2.1.12-8.el9_4?arch=x86_64&distro=rhel-9.8&upstream=libevent-2.1.12-

Red Hat Security Advisory: libevent security update

[unknown] RHSA-2026:68534 —
pkg:rpm/redhat/openshift-clients@4.17.0-202602172042.p2.gd76df14.assembly.stream.el9?arch=

Red Hat Security Advisory: OpenShift Container Platform 4.19.48 packages and security update

[unknown] RHSA-2026:68711 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:68711 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:68711 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:69125 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:69126 —
pkg:rpm/redhat/curl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.1-4

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:69126 —
pkg:rpm/redhat/libcurl-minimal@7.76.1-40.el9?arch=x86_64&distro=rhel-9.8&upstream=curl-7.76.

Red Hat Security Advisory: curl security update

[unknown] RHSA-2026:69128 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:69128 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:69128 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:69129 —

pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:69129 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:69130 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:69130 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: openssh security update

[unknown] RHSA-2026:6915 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:6915 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:69276 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:69276 —
pkg:rpm/redhat/glibc-common@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.3

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:69276 —
pkg:rpm/redhat/glibc-minimal-langpack@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:69553 —
pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:70390 —
pkg:rpm/redhat/tar@1.34-11.el9?arch=x86_64&checksum=sha256%3A58b622ab7bc225731a2473e

Red Hat Security Advisory: tar security, bug fix, and enhancement update

[unknown] RHSA-2026:70596 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:70719 —
pkg:rpm/redhat/openssh@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3Acd14a09ebe95a8d0

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:70719 —
pkg:rpm/redhat/openssh-clients@9.9p1-9.el9_8?arch=x86_64&checksum=sha256%3A2e10d31aa0

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:70818 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:70818 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:70818 —
pkg:rpm/redhat/vim-filesystem@8.2.2637-26.el9_8.13?arch=noarch&checksum=sha256%3A7758b

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:70818 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:71404 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: glib2 security update

[unknown] RHSA-2026:71542 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f42674119

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:71542 —
pkg:rpm/redhat/openssl-libs@3.5.5-6.el9_8?arch=x86_64&distro=rhel-9.8&epoch=1&upstream=ope

Red Hat Security Advisory: openssl security update

[unknown] RHSA-2026:71585 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:71586 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.13

Red Hat Security Advisory: libxml2 security update

[unknown] RHSA-2026:71655 —
pkg:rpm/redhat/expat@2.5.0-6.el9_8.1?arch=x86_64&checksum=sha256%3A6a0c98d67b643fe620

Red Hat Security Advisory: Red Hat Hardened Images RPMs Security Update

[unknown] RHSA-2026:7180 —
pkg:rpm/redhat/libblkid@2.37.4-25.el9?arch=x86_64&distro=rhel-9.8&upstream=util-linux-2.37.4-2

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7180 —
pkg:rpm/redhat/util-linux@2.37.4-25.el9?arch=x86_64&checksum=sha256%3A35e0b73e574a7d8e

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7261 —
pkg:rpm/redhat/openssl@3.5.5-6.el9_8?arch=x86_64&checksum=sha256%3A1c502507f4267411

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7263 —
pkg:rpm/redhat/ncurses@6.2-12.20210508.el9?arch=x86_64&checksum=sha256%3Ad2835ed9dbf

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7263 —
pkg:rpm/redhat/ncurses-base@6.2-12.20210508.el9?arch=noarch&distro=rhel-9.8&upstream=ncur

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7316 —
pkg:rpm/redhat/glibc@2.34-275.el9_8?arch=x86_64&distro=rhel-9.8&upstream=glibc-2.34-275.el9

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7458 —
pkg:rpm/redhat/gnupg2@2.3.3-5.el9_7?arch=x86_64&distro=rhel-9.8&upstream=gnupg2-2.3.3-5.el

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7461 —
pkg:rpm/redhat/glib2@2.68.4-19.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=glib2-2.68.4-19.

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7473 —
pkg:rpm/redhat/libcap@2.48-10.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=libcap-2.48-10.el

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7477 —
pkg:rpm/redhat/gnutls@3.8.10-8.el9_8?arch=x86_64&distro=rhel-9.8&upstream=gnutls-3.8.10-8.el

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7500 —
pkg:rpm/redhat/libtasn1@4.16.0-10.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libtasn1-4.16.0

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7519 —
pkg:rpm/redhat/libxml2@2.9.13-14.el9_8.2?arch=x86_64&distro=rhel-9.8&upstream=libxml2-2.9.1

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7545 —
pkg:rpm/redhat/oniguruma@6.9.6-1.el9.6?arch=x86_64&checksum=sha256%3Aa532fc644b41ead2

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7553 —
pkg:rpm/redhat/pam@1.5.1-28.el9?arch=x86_64&checksum=sha256%3A15a0a5000af6f57f47c306

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7578 —

pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:7666 —
pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.4

Red Hat Security Advisory: nghttp2 security update

[unknown] RHSA-2026:7711 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:7711 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053c

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:7711 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Digest@1.19-4.el9?arch=noarch&checksum=sha256%3Ae0b8633f818467f9e1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Encode@3.08-462.el9?arch=x86_64&checksum=sha256%3Ad05248697e4892

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-File-Temp@0.231.100-4.el9?arch=noarch&checksum=sha256%3A0a81b06239

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Getopt-Long@2.52-4.el9?arch=noarch&checksum=sha256%3A055fe33d2a7a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-HTTP-Tiny@0.076-462.el9?arch=noarch&checksum=sha256%3A696f388a50f

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Pod-Escapes@1.07-460.el9?arch=noarch&checksum=sha256%3A42fa08cc02a

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Pod-Simple@3.42-4.el9?arch=noarch&checksum=sha256%3A2752454ce47a4

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Pod-Usage@2.01-4.el9?arch=noarch&checksum=sha256%3Ac170870a2d1ff3

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Scalar-List-Utils@1.56-462.el9?arch=x86_64&checksum=sha256%3A7ce874b

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Socket@2.031-4.el9?arch=x86_64&checksum=sha256%3A762751146305f9ae

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Storable@3.21-460.el9?arch=x86_64&checksum=sha256%3A0097fdb40a1f83

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-Time-Local@1.300-7.el9?arch=noarch&checksum=sha256%3Ae8e1e692b6e5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-constant@1.33-461.el9?arch=noarch&checksum=sha256%3A8ab94e13cab4e7

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-interpreter@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3A929592

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-libs@5.32.1-481.1.el9_6?arch=x86_64&checksum=sha256%3Aaa0e9b31c82b5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-parent@0.238-460.el9?arch=noarch&checksum=sha256%3Aa9b2ccc25a5ed5

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8096 —
pkg:rpm/redhat/perl-podlators@4.14-460.el9?arch=noarch&checksum=sha256%3A0401f715522a1

Red Hat Security Advisory: perl:5.32 security update

[unknown] RHSA-2026:8259 —
pkg:rpm/redhat/vim-common@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A7be3f49

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:8259 —
pkg:rpm/redhat/vim-enhanced@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3A8e053

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:8259 —
pkg:rpm/redhat/vim-minimal@8.2.2637-26.el9_8.13?arch=x86_64&checksum=sha256%3Ae0ce071

Red Hat Security Advisory: vim security update

[unknown] RHSA-2026:8466 —
pkg:rpm/redhat/libgcrypt@1.10.0-13.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libgcrypt-1.10

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:8492 — pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:8579 — pkg:rpm/redhat/jq@1.6-19.el9_8.2?arch=x86_64&checksum=sha256%3A9793a39a4746a09ba89c3

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

[unknown] RHSA-2026:8865 — pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: libarchive security update

[unknown] RHSA-2026:8868 — pkg:rpm/redhat/libnghttp2@1.43.0-6.el9_8.1?arch=x86_64&distro=rhel-9.8&upstream=nghttp2-1.4

Red Hat Security Advisory: nghttp2 security update

[unknown] RHSA-2026:8944 — pkg:rpm/redhat/libarchive@3.5.3-11.el9_8?arch=x86_64&distro=rhel-9.8&upstream=libarchive-3.5.

Red Hat Security Advisory: Red Hat Hardened Images RPMs bug fix and enhancement update

Findings from inspektr_cli

[unknown] CVE-2020-8911 — pkg:golang/github.com/aws/aws-sdk-go@v1.55.6

CBC padding oracle issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2020-8911 — pkg:golang/github.com/aws/aws-sdk-go@v1.53.12

CBC padding oracle issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2020-8912 — pkg:golang/github.com/aws/aws-sdk-go@v1.55.6

In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2020-8912 — pkg:golang/github.com/aws/aws-sdk-go@v1.53.12

In-band key negotiation issue in AWS S3 Crypto SDK for golang in github.com/aws/aws-sdk-go

[unknown] CVE-2023-37264 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Pipelines do not validate child UIDs

[unknown] CVE-2023-37264 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Pipelines do not validate child UIDs

[unknown] CVE-2024-25621 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd affected by a local privilege escalation via wide permissions on CRI directory

Fixed in: 1.7.29

[unknown] CVE-2024-40635 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd has an integer overflow in User ID handling

Fixed in: 1.7.27

[unknown] CVE-2024-45310 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc can be confused to create empty files/directories on the host

Fixed in: 1.1.14

[unknown] CVE-2024-45339 — pkg:golang/github.com/golang/glog@v1.2.2

Insecure Temporary File usage in github.com/golang/glog

Fixed in: 1.2.4

[unknown] CVE-2024-5042 — pkg:golang/github.com/submariner-io/submariner-operator@v0.24.0

Submariner Operator sets unnecessary RBAC permissions in helm charts in github.com/submariner-io/submariner-operator

[unknown] CVE-2025-15558 — pkg:golang/github.com/docker/cli@v27.4.1+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows in github.com/docker/cli

Fixed in: 29.2.0+incompatible

[unknown] CVE-2025-15558 — pkg:golang/github.com/docker/cli@v28.0.0+incompatible

Docker CLI Plugins: Uncontrolled Search Path Element Leads to Local Privilege Escalation on Windows in github.com/docker/cli

Fixed in: 29.2.0+incompatible

[unknown] CVE-2025-21613 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git has an Argument Injection via the URL field

Fixed in: 5.13.0

[unknown] CVE-2025-21614 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git clients vulnerable to DoS via maliciously crafted Git server replies

Fixed in: 5.13.0

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.26.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.18.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.12.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[unknown] CVE-2025-22868 — pkg:golang/golang.org/x/oauth2@v0.23.0

golang.org/x/oauth2 Improper Validation of Syntactic Correctness of Input vulnerability

Fixed in: 0.27.0

[unknown] CVE-2025-22869 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

Fixed in: 0.35.0

[unknown] CVE-2025-22869 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto Vulnerable to Denial of Service (DoS) via Slow or Incomplete Key Exchange

Fixed in: 0.35.0

[unknown] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.33.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[unknown] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.35.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[unknown] CVE-2025-22870 — pkg:golang/golang.org/x/net@v0.34.0

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

Fixed in: 0.36.0

[unknown] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.33.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[unknown] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.35.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[unknown] CVE-2025-22872 — pkg:golang/golang.org/x/net@v0.34.0

golang.org/x/net vulnerable to Cross-site Scripting

Fixed in: 0.38.0

[unknown] CVE-2025-27144 — pkg:golang/github.com/go-jose/go-jose/v3@v3.0.3

DoS in go-jose Parsing

Fixed in: 3.0.4

[unknown] CVE-2025-30204 — pkg:golang/github.com/golang-jwt/jwt/v4@v4.5.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 4.5.2

[unknown] CVE-2025-30204 — pkg:golang/github.com/golang-jwt/jwt/v5@v5.2.1

jwt-go allows excessive memory allocation during header parsing

Fixed in: 5.2.2

[unknown] CVE-2025-31133 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc container escape via "masked path" abuse due to mount race conditions

Fixed in: 1.2.8

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.33.0

Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.35.0

Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.34.0

Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[unknown] CVE-2025-47911 — pkg:golang/golang.org/x/net@v0.41.0

Quadratic parsing complexity in golang.org/x/net/html

Fixed in: 0.45.0

[unknown] CVE-2025-47913 — pkg:golang/golang.org/x/crypto@v0.39.0

Potential denial of service in golang.org/x/crypto/ssh/agent

Fixed in: 0.43.0

[unknown] CVE-2025-47913 — pkg:golang/golang.org/x/crypto@v0.33.0

Potential denial of service in golang.org/x/crypto/ssh/agent

Fixed in: 0.43.0

[unknown] CVE-2025-47913 — pkg:golang/golang.org/x/crypto@v0.32.0

Potential denial of service in golang.org/x/crypto/ssh/agent

Fixed in: 0.43.0

[unknown] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[unknown] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[unknown] CVE-2025-47914 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh/agent vulnerable to panic if message is malformed due to out of bounds read

Fixed in: 0.45.0

[unknown] CVE-2025-52565 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc container escape with malicious config due to /dev/console mount and related races

Fixed in: 1.2.8

[unknown] CVE-2025-52881 — pkg:golang/github.com/opencontainers/selinux@v1.11.0

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.13.0

[unknown] CVE-2025-52881 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc container escape and denial of service due to arbitrary write gadgets and procfs write redirects

Fixed in: 1.2.8

[unknown] CVE-2025-54410 — pkg:golang/github.com/docker/docker@v27.4.1+incompatible

Moby firewalld reload removes bridge network isolation

Fixed in: 28.0.0

[unknown] CVE-2025-54410 — pkg:golang/github.com/docker/docker@v25.0.6+incompatible

Moby firewalld reload removes bridge network isolation

Fixed in: 25.0.13

[unknown] CVE-2025-58058 — pkg:golang/github.com/ulikunitz/xz@v0.5.11

github.com/ulikunitz/xz leaks memory when decoding a corrupted multiple LZMA archives

Fixed in: 0.5.15

[unknown] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[unknown] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[unknown] CVE-2025-58181 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto/ssh allows an attacker to cause unbounded memory consumption

Fixed in: 0.45.0

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.33.0

Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.35.0

Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.34.0

Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[unknown] CVE-2025-58190 — pkg:golang/golang.org/x/net@v0.41.0

Infinite parsing loop in golang.org/x/net

Fixed in: 0.45.0

[unknown] CVE-2025-64329 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI server: Host memory exhaustion through Attach goroutine leak

Fixed in: 1.7.29

[unknown] CVE-2025-66506 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio allocates excessive memory during token parsing

Fixed in: 1.8.3

[unknown] CVE-2025-66506 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio allocates excessive memory during token parsing

Fixed in: 1.8.3

[unknown] CVE-2025-66564 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority allocates excessive memory during request parsing

Fixed in: 2.0.3

[unknown] CVE-2025-69725 — pkg:golang/github.com/go-chi/chi@v4.1.2+incompatible

Open redirect vulnerability in the RedirectSlashes middleware in github.com/go-chi/chi

[unknown] CVE-2025-71405 — pkg:golang/github.com/go-chi/chi/v5@v5.1.0

chi Allows Host Header Injection which Leads to Open Redirect in RedirectSlashes

Fixed in: 5.2.2

[unknown] CVE-2025-8556 — pkg:golang/github.com/cloudflare/circl@v1.3.7

CIRCL-Fourq: Missing and wrong validation can lead to incorrect results

Fixed in: 1.6.1

[unknown] CVE-2026-1229 — pkg:golang/github.com/cloudflare/circl@v1.3.7

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[unknown] CVE-2026-1229 — pkg:golang/github.com/cloudflare/circl@v1.6.1

CIRCL has an incorrect calculation in secp384r1 CombinedMult

Fixed in: 1.6.3

[unknown] CVE-2026-22703 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign verification accepts any valid Rekor entry under certain conditions

Fixed in: 2.6.2

[unknown] CVE-2026-22772 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

Fixed in: 1.8.5

[unknown] CVE-2026-22772 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio is vulnerable to Server-Side Request Forgery (SSRF) via MetaIssuer Regex Bypass

Fixed in: 1.8.5

[unknown] CVE-2026-2303 — pkg:golang/go.mongodb.org/mongo-driver@v1.14.0

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

Fixed in: 1.17.7

[unknown] CVE-2026-2303 — pkg:golang/go.mongodb.org/mongo-driver@v1.16.1

mongo-go-driver has Heap Out-of-Bounds Read in GSSAPI Error Handling

Fixed in: 1.17.7

[unknown] CVE-2026-23831 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

Fixed in: 1.5.0

[unknown] CVE-2026-23831 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor's COSE v0.0.1 entry type nil pointer dereference in Canonicalize via empty Message

Fixed in: 1.5.0

[unknown] CVE-2026-23991 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf affected by client DoS via malformed server response

Fixed in: 2.3.1

[unknown] CVE-2026-23992 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf improperly validates the configured threshold for delegations

Fixed in: 2.3.1

[unknown] CVE-2026-24051 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

OpenTelemetry Go SDK Vulnerable to Arbitrary Code Execution via PATH Hijacking

Fixed in: 1.40.0

[unknown] CVE-2026-24117 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

Fixed in: 1.5.0

[unknown] CVE-2026-24117 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor affected by Server-Side Request Forgery (SSRF) via provided public key URL

Fixed in: 1.5.0

[unknown] CVE-2026-24122 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign considered signatures valid with expired intermediate certificates when transparency log verification is skipped in github.com/sigstore/cosign

[unknown] CVE-2026-24137 — pkg:golang/github.com/sigstore/sigstore@v1.8.15

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[unknown] CVE-2026-24137 — pkg:golang/github.com/sigstore/sigstore@v1.8.2

sigstore legacy TUF client allows for arbitrary file writes with target cache path traversal

Fixed in: 1.10.4

[unknown] CVE-2026-24686 — pkg:golang/github.com/theupdateframework/go-tuf/v2@v2.0.2

go-tuf Path Traversal in TAP 4 Multirepo Client Allows Arbitrary File Write via Malicious Repository Names

Fixed in: 2.4.1

[unknown] CVE-2026-25542 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

Fixed in: 1.0.2

[unknown] CVE-2026-25542 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines has VerificationPolicy regex pattern bypass via substring matching

Fixed in: 1.0.2

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.33.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.35.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.52.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.34.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[unknown] CVE-2026-25680 — pkg:golang/golang.org/x/net@v0.41.0

Go Net HTML parser is vulnerable to denial of service

Fixed in: 0.55.0

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.33.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.35.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.52.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.34.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-25681 — pkg:golang/golang.org/x/net@v0.41.0

Invoking incorrect handling of character references in DOCTYPE nodes in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-25934 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git improperly verifies data integrity values for .idx and .pack files

Fixed in: 5.16.5

[unknown] CVE-2026-25934 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git improperly verifies data integrity values for .idx and .pack files

Fixed in: 5.16.5

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.33.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.35.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.52.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.34.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-27136 — pkg:golang/golang.org/x/net@v0.41.0

Invoking duplicate attributes can cause XSS in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-27896 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

MCP Go SDK Vulnerable to Improper Handling of Case Sensitivity

Fixed in: 1.3.1

[unknown] CVE-2026-33022 — pkg:golang/github.com/tektoncd/pipeline@v0.68.0

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

Fixed in: 1.0.1

[unknown] CVE-2026-33022 — pkg:golang/github.com/tektoncd/pipeline@v0.65.1

Tekton Pipelines controller panic via long resolver name in TaskRun/PipelineRun

Fixed in: 1.0.1

[unknown] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[unknown] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[unknown] CVE-2026-33186 — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go has an authorization bypass via missing leading slash in :path

Fixed in: 1.79.3

[unknown] CVE-2026-33252 —

pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Cross-Site Tool Execution for HTTP Servers without Authorizatrion in github.com/modelcontextprotocol/go-sdk

Fixed in: 1.4.1

[unknown] CVE-2026-33540 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution affected by pull-through cache credential exfiltration via www-authenticate bearer realm

Fixed in: 3.1.0

[unknown] CVE-2026-33747 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit's Malicious frontend can cause file escape outside of storage root

Fixed in: 0.28.1

[unknown] CVE-2026-33747 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit's Malicious frontend can cause file escape outside of storage root

Fixed in: 0.28.1

[unknown] CVE-2026-33748 — pkg:golang/github.com/moby/buildkit@v0.16.0

BuildKit Git URL subdir component can cause access to restricted files

Fixed in: 0.28.1

[unknown] CVE-2026-33748 — pkg:golang/github.com/moby/buildkit@v0.12.5

BuildKit Git URL subdir component can cause access to restricted files

Fixed in: 0.28.1

[unknown] CVE-2026-33762 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git missing validation decoding Index v4 files leads to panic

Fixed in: 5.17.1

[unknown] CVE-2026-33762 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git missing validation decoding Index v4 files leads to panic

Fixed in: 5.17.1

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.33.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

Fixed in: 0.53.0

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.35.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

Fixed in: 0.53.0

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.52.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

Fixed in: 0.53.0

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.34.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

Fixed in: 0.53.0

[unknown] CVE-2026-33814 — pkg:golang/golang.org/x/net@v0.41.0

Infinite loop in HTTP/2 transport when given bad SETTINGS_MAX_FRAME_SIZE in net/http/internal/http2 in golang.org/x/net

Fixed in: 0.53.0

[unknown] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v27.4.1+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[unknown] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v25.0.6+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[unknown] CVE-2026-33997 — pkg:golang/github.com/docker/docker@v28.0.0+incompatible

Moby has an Off-by-one error in its plugin privilege validation

[unknown] CVE-2026-34040 — pkg:golang/github.com/docker/docker@v27.4.1+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies

Fixed in: 29.3.1

[unknown] CVE-2026-34040 — pkg:golang/github.com/docker/docker@v25.0.6+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies

Fixed in: 29.3.1

[unknown] CVE-2026-34040 — pkg:golang/github.com/docker/docker@v28.0.0+incompatible

Moby has AuthZ plugin bypass when provided oversized request bodies

Fixed in: 29.3.1

[unknown] CVE-2026-34165 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

Fixed in: 5.17.1

[unknown] CVE-2026-34165 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Maliciously crafted idx file can cause asymmetric memory consumption

Fixed in: 5.17.1

[unknown] CVE-2026-34742 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

DNS Rebinding Protection Disabled by Default in Model Context Protocol Go SDK for Servers Running on Localhost

Fixed in: 1.4.0

[unknown] CVE-2026-34986 — pkg:golang/github.com/go-jose/go-jose/v3@v3.0.3

Go JOSE Panics in JWE decryption

Fixed in: 3.0.5

[unknown] CVE-2026-34986 — pkg:golang/github.com/go-jose/go-jose/v4@v4.0.5

Go JOSE Panics in JWE decryption

Fixed in: 4.1.4

[unknown] CVE-2026-35172 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution: stale blob access resurrection via repo-scoped redis descriptor cache invalidation

Fixed in: 3.1.0

[unknown] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.2.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[unknown] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.4.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[unknown] CVE-2026-35469 — pkg:golang/github.com/moby/spdystream@v0.5.0

SpdyStream: DOS on CRI

Fixed in: 0.5.1

[unknown] CVE-2026-39395 — pkg:golang/github.com/sigstore/cosign/v2@v2.4.3

Cosign's verify-blob-attestation reports false positive when payload parsing fails in github.com/sigstore/cosign

Fixed in: 2.6.3

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.33.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

Fixed in: 0.55.0

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.35.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

Fixed in: 0.55.0

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.52.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

Fixed in: 0.55.0

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.34.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

Fixed in: 0.55.0

[unknown] CVE-2026-39821 — pkg:golang/golang.org/x/net@v0.41.0

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna
Fixed in: 0.55.0

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.30.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows
Fixed in: 0.44.0

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.33.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows
Fixed in: 0.44.0

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.29.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows
Fixed in: 0.44.0

[unknown] CVE-2026-39824 — pkg:golang/golang.org/x/sys@v0.42.0

Invoking integer overflow in NewNTUnicodeString in golang.org/x/sys/windows
Fixed in: 0.44.0

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39827 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking memory leak when rejecting channels can lead to DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions
Fixed in: 0.52.0

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions
Fixed in: 0.52.0

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions
Fixed in: 0.52.0

[unknown] CVE-2026-39828 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to invoking bypass of certificate restrictions

Fixed in: 0.52.0

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39829 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking pathological RSA/DSA parameters may cause DoS
Fixed in: 0.52.0

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses
Fixed in: 0.52.0

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses
Fixed in: 0.52.0

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses
Fixed in: 0.52.0

[unknown] CVE-2026-39830 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking client can cause server deadlock on unexpected responses
Fixed in: 0.52.0

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed
Fixed in: 0.52.0

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed
Fixed in: 0.52.0

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed
Fixed in: 0.52.0

[unknown] CVE-2026-39831 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: FIDO/U2F security key physical presence check can be bypassed
Fixed in: 0.52.0

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[unknown] CVE-2026-39832 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto doesn't drop invoking agent constraints when forwarding keys

Fixed in: 0.52.0

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[unknown] CVE-2026-39833 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto doesn't enforce invoking key constraints

Fixed in: 0.52.0

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[unknown] CVE-2026-39834 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to infinite loop on large channel writes

Fixed in: 0.52.0

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow
Fixed in: 0.52.0

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow
Fixed in: 0.52.0

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow
Fixed in: 0.52.0

[unknown] CVE-2026-39835 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto is vulnerable to invoking server panic during CheckHostKey/Authenticate flow
Fixed in: 0.52.0

[unknown] CVE-2026-39883 — pkg:golang/go.opentelemetry.io/otel/sdk@v1.34.0

opentelemetry-go: BSD kenv command not using absolute path enables PATH hijacking
Fixed in: 1.43.0

[unknown] CVE-2026-39984 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has Improper Certificate Validation in verifier in github.com/sigstore/timestamp-authority

[unknown] CVE-2026-41178 — pkg:golang/go.opentelemetry.io/otel@v1.43.0

Opentelemetry-go's baggage parsing no longer caps raw header length in go.opentelemetry.io/otel
Fixed in: 1.44.0

[unknown] CVE-2026-41506 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Credential leak via cross-host redirect in smart HTTP transport
Fixed in: 5.18.0

[unknown] CVE-2026-41506 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Credential leak via cross-host redirect in smart HTTP transport
Fixed in: 5.18.0

[unknown] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v27.4.1+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[unknown] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v25.0.6+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[unknown] CVE-2026-41567 — pkg:golang/github.com/docker/docker@v28.0.0+incompatible

Docker: `PUT /containers/{id}/archive` executes container binary on the host

[unknown] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v27.4.1+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[unknown] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v25.0.6+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[unknown] CVE-2026-41568 — pkg:golang/github.com/docker/docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows creation of arbitrary empty files on the host via symlink swap

[unknown] CVE-2026-41579 — pkg:golang/github.com/opencontainers/runc@v1.1.12

runc: Malicious image with /dev symlink can trigger limited host filesystem integrity violations

Fixed in: 1.3.6

[unknown] CVE-2026-41888 — pkg:golang/github.com/distribution/distribution/v3@v3.0.0-20230519140516-983358f8e250

Distribution's tag deletion bypasses `storage.delete.enabled` configuration

Fixed in: 3.1.1

[unknown] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v27.4.1+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[unknown] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v25.0.6+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[unknown] CVE-2026-42306 — pkg:golang/github.com/docker/docker@v28.0.0+incompatible

Docker: Race condition in docker cp allows bind mount redirection to host path

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.33.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.35.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.52.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.34.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42502 — pkg:golang/golang.org/x/net@v0.41.0

Invoking incorrect handling of HTML elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.33.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.35.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.52.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.34.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42506 — pkg:golang/golang.org/x/net@v0.41.0

Invoking incorrect handling of namespaced elements in foreign content in golang.org/x/net/html

Fixed in: 0.55.0

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[unknown] CVE-2026-42508 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto vulnerable to auth bypass via unenforced @revoked status

Fixed in: 0.52.0

[unknown] CVE-2026-44740 — pkg:golang/github.com/go-git/go-billy/v5@v5.5.0

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

Fixed in: 5.9.0

[unknown] CVE-2026-44740 — pkg:golang/github.com/go-git/go-billy/v5@v5.6.2

go-billy: Lack of depth and cycle detection in symlink resolution may lead to infinite loops and resource exhaustion

Fixed in: 5.9.0

[unknown] CVE-2026-44973 — pkg:golang/github.com/go-git/go-billy/v5@v5.5.0

go-billy has path traversal vulnerabilities

Fixed in: 5.9.0

[unknown] CVE-2026-44973 — pkg:golang/github.com/go-git/go-billy/v5@v5.6.2

go-billy has path traversal vulnerabilities

Fixed in: 5.9.0

[unknown] CVE-2026-45022 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

Fixed in: 5.19.0

[unknown] CVE-2026-45022 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git's improper parsing of specially crafted objects may lead to inconsistent interpretation compared to upstream Git

Fixed in: 5.19.0

[unknown] CVE-2026-45570 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Improper single-quote escaping in go-git SSH transport

Fixed in: 5.19.1

[unknown] CVE-2026-45570 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Improper single-quote escaping in go-git SSH transport

Fixed in: 5.19.1

[unknown] CVE-2026-45571 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Crafted repositories may modify main and submodule .git directories

Fixed in: 5.19.1

[unknown] CVE-2026-45571 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Crafted repositories may modify main and submodule .git directories

Fixed in: 5.19.1

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement

Fixed in: 0.52.0

[unknown] CVE-2026-46595 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking VerifiedPublicKeyCallback permissions skip enforcement
Fixed in: 0.52.0

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic
Fixed in: 0.52.0

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic
Fixed in: 0.52.0

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic
Fixed in: 0.52.0

[unknown] CVE-2026-46597 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking byte arithmetic causes underflow and panic
Fixed in: 0.52.0

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.39.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic
Fixed in: 0.52.0

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.33.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic
Fixed in: 0.52.0

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.49.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic
Fixed in: 0.52.0

[unknown] CVE-2026-46598 — pkg:golang/golang.org/x/crypto@v0.32.0

golang.org/x/crypto: Invoking pathological inputs can lead to client panic
Fixed in: 0.52.0

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.33.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage
Fixed in: 0.56.0

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.35.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage
Fixed in: 0.56.0

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.52.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage
Fixed in: 0.56.0

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.34.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

Fixed in: 0.56.0

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.55.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

Fixed in: 0.56.0

[unknown] CVE-2026-46600 — pkg:golang/golang.org/x/net@v0.41.0

Parsing an invalid SVCB or HTTPS RR can panic in golang.org/x/net/dns/dnsmessage

Fixed in: 0.56.0

[unknown] CVE-2026-47262 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd image-triggered runtime DoS via unbounded group parsing

Fixed in: 1.7.33

[unknown] CVE-2026-47262 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd image-triggered runtime DoS via unbounded group parsing

Fixed in: 1.7.33

[unknown] CVE-2026-48702 — pkg:golang/github.com/sigstore/rekor@v1.2.2

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

Fixed in: 1.5.2

[unknown] CVE-2026-48702 — pkg:golang/github.com/sigstore/rekor@v1.3.9

Rekor has an OOM Condition due to Unbounded gzip Decompression in Alpine APK Parsing Logic

Fixed in: 1.5.2

[unknown] CVE-2026-49478 — pkg:golang/github.com/sigstore/fulcio@v1.6.6

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

Fixed in: 1.8.6

[unknown] CVE-2026-49478 — pkg:golang/github.com/sigstore/fulcio@v1.4.3

Fulcio has OIDC Discovery Redirect Following Allows SSRF and JWKS Substitution for Meta-Issuer Paths, with Kubernetes Service-Account Token Leakage

Fixed in: 1.8.6

[unknown] CVE-2026-49834 — pkg:golang/github.com/sigstore/sigstore-go@v0.7.0

sigstore-go has a multi-log threshold bypass via single compromised log

Fixed in: 1.2.0

[unknown] CVE-2026-49835 — pkg:golang/github.com/sigstore/timestamp-authority@v1.2.4

Sigstore Timestamp Authority has OOM due to unbounded metric label cardinality

[unknown] CVE-2026-50163 — pkg:golang/oras.land/oras-go/v2@v2.6.1

`oras-go` tar extraction: Hardlink entry with relative Linkname escapes extract dir via process CWD resolution

Fixed in: 2.6.2

[unknown] CVE-2026-50195 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[unknown] CVE-2026-50195 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd: CRI checkpoint import allows local image tag poisoning in github.com/containerd/containerd

[unknown] CVE-2026-53488 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

Fixed in: 1.7.33

[unknown] CVE-2026-53488 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd CRI — image-config `LABEL` flows to restart-monitor `binary://` logger: host-root command execution from an image pull

Fixed in: 1.7.33

[unknown] CVE-2026-53489 — pkg:golang/github.com/containerd/containerd@v1.7.11

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[unknown] CVE-2026-53489 — pkg:golang/github.com/containerd/containerd@v1.7.32

Arbitrary host CRI log file read via symlink following in CRI checkpoint restore in github.com/containerd/containerd

[unknown] CVE-2026-53492 — pkg:golang/github.com/containerd/containerd@v1.7.11

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[unknown] CVE-2026-53492 — pkg:golang/github.com/containerd/containerd@v1.7.32

containerd CRI checkpoint restore CDI annotation smuggling in github.com/containerd/containerd

[unknown] CVE-2026-54787 — pkg:golang/github.com/sigstore/sigstore-go@v0.7.0

sigstore-go fails to check signature timestamps against a signing key's validity period

Fixed in: 1.2.1

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.35.0

Infinite loop on invalid input in golang.org/x/text

Fixed in: 0.39.0

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.37.0?type=module

Infinite loop on invalid input in golang.org/x/text

Fixed in: 0.39.0

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.22.0

Infinite loop on invalid input in golang.org/x/text

Fixed in: 0.39.0

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.26.0

Infinite loop on invalid input in golang.org/x/text

Fixed in: 0.39.0

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.38.0

Infinite loop on invalid input in golang.org/x/text

Fixed in: 0.39.0

[unknown] CVE-2026-56852 — pkg:golang/golang.org/x/text@v0.21.0

Infinite loop on invalid input in golang.org/x/text

Fixed in: 0.39.0

[unknown] CVE-2026-56864 — pkg:golang/golang.org/x/mod@v0.22.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

Fixed in: 0.40.0

[unknown] CVE-2026-56864 — pkg:golang/golang.org/x/mod@v0.25.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

Fixed in: 0.40.0

[unknown] CVE-2026-56864 — pkg:golang/golang.org/x/mod@v0.33.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

Fixed in: 0.40.0

[unknown] CVE-2026-56865 — pkg:golang/golang.org/x/mod@v0.22.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

Fixed in: 0.40.0

[unknown] CVE-2026-56865 — pkg:golang/golang.org/x/mod@v0.25.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

Fixed in: 0.40.0

[unknown] CVE-2026-56865 — pkg:golang/golang.org/x/mod@v0.33.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

Fixed in: 0.40.0

[unknown] CVE-2026-71556 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Worktree operations may follow symlinks

Fixed in: 5.19.2

[unknown] CVE-2026-71556 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Worktree operations may follow symlinks

Fixed in: 5.19.2

[unknown] CVE-2026-71557 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Malicious reference names may modify files outside the reference storage

Fixed in: 5.19.2

[unknown] CVE-2026-71557 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Malicious reference names may modify files outside the reference storage

Fixed in: 5.19.2

[unknown] CVE-2026-72816 — pkg:golang/github.com/go-chi/chi/v5@v5.1.0

Chi's RealIP Middleware allows IP spoofing via unvalidated X-Forwarded-For header in github.com/go-chi/chi

Fixed in: 5.3.0

[unknown] CVE-2026-72817 — pkg:golang/github.com/go-chi/chi/v5@v5.1.0

Chi Middleware vulnerable to IP spoofing via X-Forwarded-For header in github.com/go-chi/chi

Fixed in: 5.3.0

[unknown] GHSA-gcjh-h69q-9w9g — pkg:golang/github.com/google/cel-go@v0.23.2

cel-go: JSON Private Fields Exposed via NativeTypes and ParseStructTag

Fixed in: 0.29.0

[unknown] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.70.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[unknown] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.67.1

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[unknown] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.80.0

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[unknown] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.79.3

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[unknown] GHSA-hrxh-6v49-42gf — pkg:golang/google.golang.org/grpc@v1.69.4

gRPC-Go: xDS RBAC and HTTP/2 Vulnerabilities

Fixed in: 1.82.1

[unknown] GHSA-pmwq-pjrm-6p5r — pkg:golang/github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior

Fixed in: 0.11.0

[unknown] GHSA-q382-vc8q-7jhj — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

Fixed in: 1.4.1

[unknown] GHSA-w5pp-99ch-qj29 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

go-git: Malformed Git object data may cause panics or resource exhaustion

Fixed in: 5.19.1

[unknown] GHSA-w5pp-99ch-qj29 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

go-git: Malformed Git object data may cause panics or resource exhaustion

Fixed in: 5.19.1

[unknown] GHSA-xmrv-pmrh-hhx2 — pkg:golang/github.com/aws/aws-sdk-go-v2/service/s3@v1.76.0

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

Fixed in: 1.97.3

[unknown] GHSA-xmrv-pmrh-hhx2 — pkg:golang/github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream@v1.6.8

Denial of Service due to Panic in AWS SDK for Go v2 SDK EventStream Decoder

Fixed in: 1.7.8

[unknown] GO-2026-4770 — pkg:golang/github.com/modelcontextprotocol/go-sdk@v1.1.0

Improper handling of null Unicode character when parsing JSON in github.com/modelcontextprotocol/go-sdk

Fixed in: 1.4.1

[unknown] GO-2026-5547 — pkg:golang/github.com/in-toto/in-toto-golang@v0.9.1-0.20240317085821-8e2966059a09

in-toto-golang and in-toto-python have inconsistent negation behavior in github.com/in-toto/in-toto-golang

Fixed in: 0.11.0

[unknown] GO-2026-5693 — pkg:golang/github.com/go-git/go-git/v5@v5.13.2

Go-git: Malformed Git object data may cause panics or resource exhaustion in github.com/go-git/go-git

Fixed in: 5.19.1

[unknown] GO-2026-5693 — pkg:golang/github.com/go-git/go-git/v5@v5.11.0

Go-git: Malformed Git object data may cause panics or resource exhaustion in github.com/go-git/go-git

Fixed in: 5.19.1

[unknown] GO-2026-5764 — pkg:golang/github.com/aws/aws-sdk-go-v2/service/s3@v1.76.0

DoS due to Panic in AWS SDK for Go v2 SDK EventStream Decoder in github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream

Fixed in: 1.97.3

[unknown] GO-2026-5764 — pkg:golang/github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream@v1.6.8

DoS due to Panic in AWS SDK for Go v2 SDK EventStream Decoder in github.com/aws/aws-sdk-go-v2/aws/protocol/eventstream

Fixed in: 1.7.8

[unknown] GO-2026-5841 — pkg:golang/github.com/klauspost/compress@v1.18.4

OOB read in github.com/klauspost/compress/s2

Fixed in: 1.18.7

[unknown] GO-2026-5841 — pkg:golang/github.com/klauspost/compress@v1.17.11

OOB read in github.com/klauspost/compress/s2

Fixed in: 1.18.7

[unknown] GO-2026-5841 — pkg:golang/github.com/klauspost/compress@v1.17.7

OOB read in github.com/klauspost/compress/s2

Fixed in: 1.18.7

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.39.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.33.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.49.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.32.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.53.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.70.0

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

Fixed in: 1.82.1

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.67.1

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

Fixed in: 1.82.1

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.80.0

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

Fixed in: 1.82.1

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.79.3

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

Fixed in: 1.82.1

[unknown] GO-2026-6061 — pkg:golang/google.golang.org/grpc@v1.69.4

Vulnerabilities in the xDS RBAC authorization engine and the HTTP/2 transport server implementation in google.golang.org/grpc

Fixed in: 1.82.1

Skipped or failed analyzers

shieldbom (fail): Parsed 2813 components from "/tmp/sba-analyze-177915-2912-17903541512121475 91-14/input.spdx.json" (SPDX 2.3 (JSON)) Found 31 vulnerabilities Found 2813 license issues DISCLAIMER: This report is provided "AS IS" without warranty of any kind. Vulnerability results are based on publicly available data sources (e.g., OSV.dev, NVD) which may be incomplete or delayed. The absence of reported vulnerabilities does not guarantee that the software is free of security issues. This tool assists with security analysis but does not constitute a complete security assessment, legal advice, or certification of regulatory compliance (including EU CRA conformity). Users are solely responsible for their own compliance determinations. Always perform additional security assessments as appropriate.