

ndaal SBOM Auditor — analysis of k8s-v1.37.0-source.spdx (SBOM #1938)

SBOM metadata

Name: k8s-v1.37.0-source.spdx * Format: spdx-tag

Spec version: SPDX-2.3 * Components: 169 * Source: upload

SHA-256: 24022414edc9c0b8942864fe174e82f746c3993800b6e278ac772f587e0437c7

Ingested: 2026-09-05T09:55:11Z

Analyzer summary

syft 1.51.0 — ok — 0 finding(s)

grype 0.118.0 — ok — 9 finding(s)

trivy 0.74.0 — ok — 3 finding(s)

osv-scanner 2.5.1 — ok — 163 finding(s)

bomber 0.5.1 — ok — 12 finding(s)

bomdrift bomdrift 0.9.9 — fail — 0 finding(s)

inspektr_cli inspektr 0.1.9 — fail — 0 finding(s)

shieldbom shieldbom 0.3.0 — fail — 0 finding(s)

provenant provenant-cli 1.0.8 — ok — 0 finding(s)

Findings from grype

[high] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — google.golang.org/grpc@v1.82.1

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

Fixed in: 1.83.1

[high] GO-2026-6107 (CVE-2026-73500) — go.etcd.io/etcd/client/pkg/v3@v3.7.0

In go.etcd.io/etcd/client/pkg/v3 before 3.5.33, 3.6.14, and 3.7.1, TLS handshakes on listeners created by NewTLSListener do not enforce a handshake deadline. An unauthenticated network attacker who connects to an etcd TLS listener without sending a ClientHello causes a goroutine and a tracking map entry to block indefinitely. Opening many such connections exhausts memory, leading to a denial of service.

Fixed in: 3.5.33

[high] GO-2026-6114 (CVE-2026-73499) — go.etcd.io/etcd/server/v3@v3.7.0

In go.etcd.io/etcd/server/v3 before 3.5.33, 3.6.14, and 3.7.1, an authenticated user with READ permission on a single key can bypass RBAC restrictions by initiating an open-ended range watch using clientv3.WithFromKey(). The Watch RPC handler normalized open-ended range ends prior to authorization checks, causing isWatchPermitted to evaluate the request as a single-key watch while the underlying watch stream received events for all keys lexicographically greater than or equal to the target key.

Fixed in: 3.5.33

[high] GO-2026-6179 (CVE-2026-56865) — golang.org/x/mod@v0.37.0

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@v0.37.0](#)

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@v0.54.0](#)

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@v0.54.0](#)

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@v0.54.0](#)

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

[unknown] GO-2026-5932 — [golang.org/x/crypto@v0.54.0](#)

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.

Findings from trivy

[high] CVE-2026-56864 — [golang.org/x/mod@v0.37.0](#)

A malicious GOSUMDB was capable of serving arbitrary module content no ...

Fixed in: 0.40.0

[high] CVE-2026-56865 — [golang.org/x/mod@v0.37.0](#)

A malicious GOPROXY was previously capable of forging up to two sumdb ...

Fixed in: 0.40.0

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.54.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

Findings from osv-scanner

[unknown] GHSA-2v4p-qf9q-27wj (CVE-2026-84445) — grpc@v1.82.1

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

[unknown] GHSA-qc2q-p7wx-3px3 (CVE-2026-84303) — grpc@v1.82.1

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] GHSA-vp52-pcj8-j9qc (CVE-2026-84304) — grpc@v1.82.1

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

[unknown] GO-2021-0142 (CVE-2020-16845) — stdlib@v1.1.12

Unbounded read from invalid inputs in encoding/binary

[unknown] GO-2021-0154 (CVE-2014-7189) — stdlib@v1.1.12

Man-in-the-middle attack with SessionTicketsDisabled in crypto/tls

[unknown] GO-2021-0159 (CVE-2015-5739) — stdlib@v1.1.12

Request smuggling due to improper header parsing in net/http

[unknown] GO-2021-0163 (CVE-2016-3958) — stdlib@v1.1.12

Privilege escalation on Windows via malicious DLL in syscall

[unknown] GO-2021-0172 (CVE-2017-1000098) — stdlib@v1.1.12

Denial of service when parsing large forms in mime/multipart

[unknown] GO-2021-0178 (CVE-2017-15042) — stdlib@v1.1.12

Cleartext transmission of credentials in net/smtp

[unknown] GO-2021-0223 (CVE-2020-14039) — stdlib@v1.1.12

Certificate verification error on Windows in crypto/x509

[unknown] GO-2021-0224 (CVE-2020-15586) — stdlib@v1.1.12

Data race and crash in net/http

[unknown] GO-2021-0226 (CVE-2020-24553) — stdlib@v1.1.12

Cross-site scripting in net/http/cgi and net/http/cgi

[unknown] GO-2021-0234 (CVE-2021-27918) — stdlib@v1.1.12

Infinite loop when decoding inputs in encoding/xml

[unknown] GO-2021-0235 (CVE-2021-3114) — stdlib@v1.1.12

Incorrect operations on the P-224 curve in crypto/elliptic

[unknown] GO-2021-0239 (CVE-2021-33195) — stdlib@v1.1.12

Improper sanitization when resolving values from DNS in net

[unknown] GO-2021-0240 (CVE-2021-33196) – stdlib@v1.1.12

Panic when reading certain archives in archive/zip

[unknown] GO-2021-0241 (CVE-2021-33197) – stdlib@v1.1.12

Attacker can drop certain headers in net/http/httputil

[unknown] GO-2021-0242 (CVE-2021-33198) – stdlib@v1.1.12

Panic on inputs with large exponents in math/big

[unknown] GO-2021-0243 (CVE-2021-34558) – stdlib@v1.1.12

Panic on certain certificates in crypto/tls

[unknown] GO-2021-0245 (CVE-2021-36221) – stdlib@v1.1.12

Panic in ReverseProxy in net/http/httputil

[unknown] GO-2021-0263 (CVE-2021-41771) – stdlib@v1.1.12

Panic on invalid symbol tables in debug/macho

[unknown] GO-2021-0264 (CVE-2021-41772) – stdlib@v1.1.12

Panic when opening certain archives in archive/zip

[unknown] GO-2021-0317 (CVE-2022-23772) – stdlib@v1.1.12

Uncontrolled memory consumption in math/big

[unknown] GO-2021-0319 (CVE-2022-23806) – stdlib@v1.1.12

Incorrect computation for some invalid field elements in crypto/elliptic

[unknown] GO-2021-0347 (CVE-2022-24921) – stdlib@v1.1.12

Stack exhaustion when compiling deeply nested expressions in regexp

[unknown] GO-2022-0166 (CVE-2016-3959) – stdlib@v1.1.12

Denial of service due to unchecked parameters in crypto/dsa

[unknown] GO-2022-0171 (CVE-2017-1000097) – stdlib@v1.1.12

Mishandled trust preferences for root certificates on Darwin in crypto/x509

[unknown] GO-2022-0191 (CVE-2018-16875) – stdlib@v1.1.12

Denial of service in chain verification in crypto/x509

[unknown] GO-2022-0211 (CVE-2019-14809) – stdlib@v1.1.12

Incorrect parsing validation in net/url

[unknown] GO-2022-0212 (CVE-2019-16276) – stdlib@v1.1.12

Request smuggling due to accepting invalid headers in net/http via net/textproto

[unknown] GO-2022-0213 (CVE-2019-17596) – stdlib@v1.1.12

Panic on invalid DSA public keys in crypto/dsa

[unknown] GO-2022-0217 (CVE-2019-6486) – stdlib@v1.1.12

Denial of service affecting P-521 and P-384 curves in crypto/elliptic

[unknown] GO-2022-0220 (CVE-2019-9634) – stdlib@v1.1.12

DLL injection on Windows in runtime and syscall

[unknown] GO-2022-0229 (CVE-2020-7919) – stdlib@v1.1.12

Panic in certificate parsing in crypto/x509 and golang.org/x/crypto/cryptobyte

[unknown] GO-2022-0236 (CVE-2021-31525) – stdlib@v1.1.12

Panic due to large headers in net/http and golang.org/x/net/http/httpguts

[unknown] GO-2022-0273 (CVE-2021-39293) – stdlib@v1.1.12

Panic due to crafted inputs in archive/zip

[unknown] GO-2022-0288 (CVE-2021-44716) – stdlib@v1.1.12

Unbounded memory growth in net/http and golang.org/x/net/http2

[unknown] GO-2022-0289 (CVE-2021-44717) – stdlib@v1.1.12

Misdirected I/O in syscall

[unknown] GO-2022-0433 (CVE-2022-24675) – stdlib@v1.1.12

Stack overflow from a large amount of PEM data in encoding/pem

[unknown] GO-2022-0435 (CVE-2022-28327) – stdlib@v1.1.12

Panic due to large inputs affecting P-256 curves in crypto/elliptic

[unknown] GO-2022-0477 (CVE-2022-30634) – stdlib@v1.1.12

Indefinite hang with large buffers on Windows in crypto/rand

[unknown] GO-2022-0493 (CVE-2022-29526) – stdlib@v1.1.12

Incorrect privilege reporting in syscall and golang.org/x/sys/unix

[unknown] GO-2022-0515 (CVE-2022-1962) – stdlib@v1.1.12

Stack exhaustion due to deeply nested types in go/parser

[unknown] GO-2022-0520 (CVE-2022-32148) – stdlib@v1.1.12

Exposure of client IP addresses in net/http

[unknown] GO-2022-0521 (CVE-2022-28131) – stdlib@v1.1.12

Stack exhaustion from deeply nested XML documents in encoding/xml

[unknown] GO-2022-0522 (CVE-2022-30632) – stdlib@v1.1.12

Stack exhaustion on crafted paths in path/filepath

[unknown] GO-2022-0523 (CVE-2022-30633) – stdlib@v1.1.12

Stack exhaustion when unmarshaling certain documents in encoding/xml

[unknown] GO-2022-0524 (CVE-2022-30631) – stdlib@v1.1.12

Stack exhaustion when reading certain archives in compress/gzip

[unknown] GO-2022-0525 (CVE-2022-1705) – stdlib@v1.1.12

Improper sanitization of Transfer-Encoding headers in net/http

[unknown] GO-2022-0526 (CVE-2022-30635) – stdlib@v1.1.12

Stack exhaustion when decoding certain messages in encoding/gob

[unknown] GO-2022-0527 (CVE-2022-30630) – stdlib@v1.1.12

Stack exhaustion in Glob on certain paths in io/fs

[unknown] GO-2022-0531 (CVE-2022-30629) – stdlib@v1.1.12

Session tickets lack random ticket_age_add in crypto/tls

[unknown] GO-2022-0532 (CVE-2022-30580) – stdlib@v1.1.12

Empty Cmd.Path can trigger unintended binary in os/exec on Windows

[unknown] GO-2022-0533 (CVE-2022-29804) – stdlib@v1.1.12

Path traversal via Clean on Windows in path/filepath

[unknown] GO-2022-0535 (CVE-2020-0601) – stdlib@v1.1.12

Certificate validation bypass on Windows in crypto/x509

[unknown] GO-2022-0536 (CVE-2019-9512) – stdlib@v1.1.12

Reset flood in net/http and golang.org/x/net/http

[unknown] GO-2022-0537 (CVE-2022-32189) – stdlib@v1.1.12

Panic when decoding Float and Rat types in math/big

[unknown] GO-2022-0761 (CVE-2016-5386) – stdlib@v1.1.12

Improper input validation in net/http and net/http/cgi

[unknown] GO-2022-0969 (CVE-2022-27664) – stdlib@v1.1.12

Denial of service in net/http and golang.org/x/net/http2

[unknown] GO-2022-1037 (CVE-2022-2879) – stdlib@v1.1.12

Unbounded memory consumption when reading headers in archive/tar

[unknown] GO-2022-1038 (CVE-2022-2880) – stdlib@v1.1.12

Incorrect sanitization of forwarded query parameters in net/http/httputil

[unknown] GO-2022-1039 (CVE-2022-41715) – stdlib@v1.1.12

Memory exhaustion when compiling regular expressions in regexp/syntax

[unknown] GO-2022-1095 (CVE-2022-41716) – stdlib@v1.1.12

Unsanitized NUL in environment variables on Windows in syscall and os/exec

[unknown] GO-2022-1143 (CVE-2022-41720) – stdlib@v1.1.12

Restricted file access on Windows in os and net/http

[unknown] GO-2022-1144 (CVE-2022-41717) – stdlib@v1.1.12

Excessive memory growth in net/http and golang.org/x/net/http2

[unknown] GO-2023-1568 (CVE-2022-41722) – stdlib@v1.1.12

Path traversal on Windows in path/filepath

[unknown] GO-2023-1569 (CVE-2022-41725) – stdlib@v1.1.12

Excessive resource consumption in mime/multipart

[unknown] GO-2023-1570 (CVE-2022-41724) – stdlib@v1.1.12

Panic on large handshake records in crypto/tls

[unknown] GO-2023-1571 (CVE-2022-41723) – stdlib@v1.1.12

Denial of service via crafted HTTP/2 stream in net/http and golang.org/x/net

[unknown] GO-2023-1621 (CVE-2023-24532) – stdlib@v1.1.12

Incorrect calculation on P256 curves in crypto/internal/nistec

[unknown] GO-2023-1702 (CVE-2023-24537) – stdlib@v1.1.12

Infinite loop in parsing in go/scanner

[unknown] GO-2023-1703 (CVE-2023-24538) – stdlib@v1.1.12

Backticks not treated as string delimiters in html/template

[unknown] GO-2023-1704 (CVE-2023-24534) – stdlib@v1.1.12

Excessive memory allocation in net/http and net/textproto

[unknown] GO-2023-1705 (CVE-2023-24536) – stdlib@v1.1.12

Excessive resource consumption in net/http, net/textproto and mime/multipart

[unknown] GO-2023-1751 (CVE-2023-24539) – stdlib@v1.1.12

Improper sanitization of CSS values in html/template

[unknown] GO-2023-1752 (CVE-2023-24540) – stdlib@v1.1.12

Improper handling of JavaScript whitespace in html/template

[unknown] GO-2023-1753 (CVE-2023-29400) – stdlib@v1.1.12

Improper handling of empty HTML attributes in html/template

[unknown] GO-2023-1840 (CVE-2023-29403) – stdlib@v1.1.12

Unsafe behavior in setuid/setgid binaries in runtime

[unknown] GO-2023-1878 (CVE-2023-29406) – stdlib@v1.1.12

Insufficient sanitization of Host header in net/http

[unknown] GO-2023-1987 (CVE-2023-29409) – stdlib@v1.1.12

Large RSA keys can cause high CPU usage in crypto/tls

[unknown] GO-2023-2041 (CVE-2023-39318) – stdlib@v1.1.12

Improper handling of HTML-like comments in script contexts in html/template

[unknown] GO-2023-2043 (CVE-2023-39319) – stdlib@v1.1.12

Improper handling of special tags within script contexts in html/template

[unknown] GO-2023-2102 (CVE-2023-39325) – stdlib@v1.1.12

HTTP/2 rapid reset can cause excessive work in net/http

[unknown] GO-2023-2185 (CVE-2023-45283) – stdlib@v1.1.12

Insecure parsing of Windows paths with a \\?\\ prefix in path/filepath

[unknown] GO-2023-2186 (CVE-2023-45284) – stdlib@v1.1.12

Incorrect detection of reserved device names on Windows in path/filepath

[unknown] GO-2023-2375 (CVE-2023-45287) – stdlib@v1.1.12

Before Go 1.20, the RSA based key exchange methods in crypto/tls may exhibit a timing side channel

[unknown] GO-2023-2382 (CVE-2023-39326) – stdlib@v1.1.12

Denial of service via chunk extensions in net/http

[unknown] GO-2024-2598 (CVE-2024-24783) – stdlib@v1.1.12

Verify panics on certificates with an unknown public key algorithm in crypto/x509

[unknown] GO-2024-2599 (CVE-2023-45290) – stdlib@v1.1.12

Memory exhaustion in multipart form parsing in net/textproto and net/http

[unknown] GO-2024-2600 (CVE-2023-45289) – stdlib@v1.1.12

Incorrect forwarding of sensitive headers and cookies on HTTP redirect in net/http

[unknown] GO-2024-2609 (CVE-2024-24784) – stdlib@v1.1.12

Comments in display names are incorrectly handled in net/mail

[unknown] GO-2024-2610 (CVE-2024-24785) – stdlib@v1.1.12

Errors returned from JSON marshaling may break template escaping in html/template

[unknown] GO-2024-2687 (CVE-2023-45288) – stdlib@v1.1.12

HTTP/2 CONTINUATION flood in net/http

[unknown] GO-2024-2887 (CVE-2024-24790) – stdlib@v1.1.12

Unexpected behavior from Is methods for IPv4-mapped IPv6 addresses in net/netip

[unknown] GO-2024-2888 (CVE-2024-24789) – stdlib@v1.1.12

Mishandling of corrupt central directory record in archive/zip

[unknown] GO-2024-2963 (CVE-2024-24791) – stdlib@v1.1.12

Denial of service due to improper 100-continue handling in net/http

[unknown] GO-2024-3105 (CVE-2024-34155) – stdlib@v1.1.12

Stack exhaustion in all Parse functions in go/parser

[unknown] GO-2024-3106 (CVE-2024-34156) – stdlib@v1.1.12

Stack exhaustion in Decoder.Decode in encoding/gob

[unknown] GO-2024-3107 (CVE-2024-34158) – stdlib@v1.1.12

Stack exhaustion in Parse in go/build/constraint

[unknown] GO-2025-3373 (CVE-2024-45341) – stdlib@v1.1.12

Usage of IPv6 zone IDs can bypass URI name constraints in crypto/x509

[unknown] GO-2025-3420 (CVE-2024-45336) – stdlib@v1.1.12

Sensitive headers incorrectly sent after cross-domain redirect in net/http

[unknown] GO-2025-3447 (CVE-2025-22866) – stdlib@v1.1.12

Timing sidechannel for P-256 on ppc64le in crypto/internal/nistec

[unknown] GO-2025-3503 (CVE-2025-22870) – stdlib@v1.1.12

HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

[unknown] GO-2025-3563 (CVE-2025-22871) – stdlib@v1.1.12

Request smuggling due to acceptance of invalid chunked data in net/http

[unknown] GO-2025-3750 (CVE-2025-0913) – stdlib@v1.1.12

Inconsistent handling of O_CREATE|O_EXCL on Unix and Windows in os in syscall

[unknown] GO-2025-3751 (CVE-2025-4673) – stdlib@v1.1.12

Sensitive headers not cleared on cross-origin redirect in net/http

[unknown] GO-2025-3849 (CVE-2025-47907) – stdlib@v1.1.12

Incorrect results returned from Rows.Scan in database/sql

[unknown] GO-2025-3956 (CVE-2025-47906) – stdlib@v1.1.12

Unexpected paths returned from LookPath in os/exec

[unknown] GO-2025-4006 (CVE-2025-61725) – stdlib@v1.1.12

Excessive CPU consumption in ParseAddress in net/mail

[unknown] GO-2025-4007 (CVE-2025-58187) – stdlib@v1.1.12

Quadratic complexity when checking name constraints in crypto/x509

[unknown] GO-2025-4008 (CVE-2025-58189) – stdlib@v1.1.12

ALPN negotiation error contains attacker controlled information in crypto/tls

[unknown] GO-2025-4009 (CVE-2025-61723) – stdlib@v1.1.12

Quadratic complexity when parsing some invalid inputs in encoding/pem

[unknown] GO-2025-4010 (CVE-2025-47912) – stdlib@v1.1.12

Insufficient validation of bracketed IPv6 hostnames in net/url

[unknown] GO-2025-4011 (CVE-2025-58185) – stdlib@v1.1.12

Parsing DER payload can cause memory exhaustion in encoding/asn1

[unknown] GO-2025-4012 (CVE-2025-58186) – stdlib@v1.1.12

Lack of limit when parsing cookies can cause memory exhaustion in net/http

[unknown] GO-2025-4013 (CVE-2025-58188) – stdlib@v1.1.12

Panic when validating certificates with DSA public keys in crypto/x509

[unknown] GO-2025-4014 (CVE-2025-58183) – stdlib@v1.1.12

Unbounded allocation when parsing GNU sparse map in archive/tar

[unknown] GO-2025-4015 (CVE-2025-61724) – stdlib@v1.1.12

Excessive CPU consumption in Reader.ReadResponse in net/textproto

[unknown] GO-2025-4155 (CVE-2025-61729) – stdlib@v1.1.12

Excessive resource consumption when printing error string for host certificate validation in crypto/x509

[unknown] GO-2025-4175 (CVE-2025-61727) – stdlib@v1.1.12

Improper application of excluded DNS name constraints when verifying wildcard names in crypto/x509

[unknown] GO-2026-4337 (CVE-2025-68121) – stdlib@v1.1.12

Unexpected session resumption in crypto/tls

[unknown] GO-2026-4340 (CVE-2025-61730) – stdlib@v1.1.12

Handshake messages may be processed at the incorrect encryption level in crypto/tls

[unknown] GO-2026-4341 (CVE-2025-61726) – stdlib@v1.1.12

Memory exhaustion in query parameter parsing in net/url

[unknown] GO-2026-4342 (CVE-2025-61728) – stdlib@v1.1.12

Excessive CPU consumption when building archive index in archive/zip

[unknown] GO-2026-4403 (CVE-2025-22873) – stdlib@v1.1.12

Improper access to parent directory of root in os

[unknown] GO-2026-4601 (CVE-2026-25679) – stdlib@v1.1.12

Incorrect parsing of IPv6 host literals in net/url

[unknown] GO-2026-4602 (CVE-2026-27139) – stdlib@v1.1.12

FileInfo can escape from a Root in os

[unknown] GO-2026-4603 (CVE-2026-27142) – stdlib@v1.1.12

URLs in meta content attribute actions are not escaped in html/template

[unknown] GO-2026-4864 (CVE-2026-32282) – stdlib@v1.1.12

TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

[unknown] GO-2026-4865 (CVE-2026-32289) – stdlib@v1.1.12

JsBraceDepth Context Tracking Bugs (XSS) in html/template

[unknown] GO-2026-4869 (CVE-2026-32288) – stdlib@v1.1.12

Unbounded allocation for old GNU sparse in archive/tar

[unknown] GO-2026-4870 (CVE-2026-32283) – stdlib@v1.1.12

Unauthenticated TLS 1.3 KeyUpdate record can cause persistent connection retention and DoS in crypto/tls

[unknown] GO-2026-4918 (CVE-2026-33814) – stdlib@v1.1.12

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-2026-4946 (CVE-2026-32281) – stdlib@v1.1.12

Inefficient policy validation in crypto/x509

[unknown] GO-2026-4947 (CVE-2026-32280) – stdlib@v1.1.12

Unexpected work during chain building in crypto/x509

[unknown] GO-2026-4970 (CVE-2026-39822) – stdlib@v1.1.12

Root escape via symlink plus trailing slash in os

[unknown] GO-2026-4971 (CVE-2026-39836) – stdlib@v1.1.12

Panic in Dial and LookupPort when handling NUL byte on Windows in net

[unknown] GO-2026-4976 (CVE-2026-39825) – stdlib@v1.1.12

ReverseProxy forwards queries with more than urlmaxqueryparams parameters in net/http/httputil

[unknown] GO-2026-4977 (CVE-2026-42499) – stdlib@v1.1.12

Quadratic string concatenation in consumePhrase in net/mail

[unknown] GO-2026-4980 (CVE-2026-39826) – stdlib@v1.1.12

Escaper bypass leads to XSS in html/template

[unknown] GO-2026-4981 (CVE-2026-33811) – stdlib@v1.1.12

Crash when handling long CNAME response in net

[unknown] GO-2026-4982 (CVE-2026-39823) – stdlib@v1.1.12

Bypass of meta content URL escaping causes XSS in html/template

[unknown] GO-2026-4986 (CVE-2026-39820) – stdlib@v1.1.12

Quadratic string concatenation in consumeComment in net/mail

[unknown] GO-2026-5026 (CVE-2026-39821) – stdlib@v1.1.12

Invoking failure to reject ASCII-only Punycode-encoded labels in golang.org/x/net/idna

[unknown] GO-2026-5037 (CVE-2026-27145) – stdlib@v1.1.12

Inefficient candidate hostname parsing in crypto/x509

[unknown] GO-2026-5038 (CVE-2026-42504) – stdlib@v1.1.12

Quadratic complexity in WordDecoder.DecodeHeader in mime

[unknown] GO-2026-5039 (CVE-2026-42507) – stdlib@v1.1.12

Arbitrary inputs are included in errors without any escaping in net/textproto

[unknown] GO-2026-5856 (CVE-2026-42505) – stdlib@v1.1.12

Invoking Encrypted Client Hello privacy leak in crypto/tls

[unknown] GO-2026-5932 – crypto@v0.54.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-5972 (CVE-2026-33818) – stdlib@v1.1.12

Enforce maximum recursion depth in encoding/asn1

[unknown] GO-2026-6088 (CVE-2026-56859) – stdlib@v1.1.12

Add recursion depth guard during decode in encoding/xml

[unknown] GO-2026-6089 (CVE-2026-56853) – stdlib@v1.1.12

Apply ReadHeaderTimeout when doing unencrypted HTTP/2 check in net/http

[unknown] GO-2026-6090 (CVE-2026-56862) – stdlib@v1.1.12

Limit handshake messages we are willing to accept post-handshake in crypto/tls

[unknown] GO-2026-6091 (CVE-2026-56858) – stdlib@v1.1.12

Fix Javascript regexp context tracking in html/template

[unknown] GO-2026-6094 – cel-go@v0.29.2

JSON private fields exposed via NativeTypes and ParseStructTag in github.com/google/cel-go

[unknown] GO-2026-6107 (CVE-2026-73500) – v3@v3.7.0

Unbounded TLS handshake goroutines in go.etcd.io/etcd/client/pkg/v3

[unknown] GO-2026-6114 (CVE-2026-73499) – v3@v3.7.0

Watch API authorization bypass in go.etcd.io/etcd/server/v3

[unknown] GO-2026-6179 (CVE-2026-56865) – mod@v0.37.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] GO-2026-6180 (CVE-2026-56864) – mod@v0.37.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] GO-2026-6218 (CVE-2026-56860) – stdlib@v1.1.12

Avoid quadratic complexity in resolvePath in net/url

[unknown] GO-2026-6303 (CVE-2026-56854) – crypto@v0.54.0

Source-address critical option not enforced for non-public-key auth callbacks in golang.org/x/crypto/ssh

[unknown] GO-2026-6354 (CVE-2026-78662) – crypto@v0.54.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-6355 (CVE-2026-56855) – crypto@v0.54.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

Findings from bomber

[high] CVE-2026-84304 – pkg:golang/google.golang.org/grpc@v1.82.1

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

[high] CVE-2026-84445 – pkg:golang/google.golang.org/grpc@v1.82.1

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

[medium] CVE-2026-84303 – pkg:golang/google.golang.org/grpc@v1.82.1

gRPC-Go: xDS RBAC HTTP Filter bypass via mixed-case Header Matching and gRFC A41 validation evasion

[unknown] CVE-2026-56854 – pkg:golang/golang.org/x/crypto@v0.54.0

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@v0.54.0

Prevent DoS on deadlocked established channel in golang.org/x/crypto/ssh

[unknown] CVE-2026-56864 – pkg:golang/golang.org/x/mod@v0.37.0

Ignore unrelated, unauthenticated hashes in Lookup in golang.org/x/mod/sumdb

[unknown] CVE-2026-56865 – pkg:golang/golang.org/x/mod@v0.37.0

Fix transparency log tile verification bypass in golang.org/x/mod/sumdb/tlog

[unknown] CVE-2026-73499 – pkg:golang/go.etcd.io/etcd/server/v3@v3.7.0

Watch API authorization bypass in go.etcd.io/etcd/server/v3

[unknown] CVE-2026-73500 — pkg:golang/go.etcd.io/etcd/client/pkg/v3@v3.7.0

Unbounded TLS handshake goroutines in go.etcd.io/etcd/client/pkg/v3

[unknown] CVE-2026-78662 — pkg:golang/golang.org/x/crypto@v0.54.0

Prevent DoS on deadlocked undecided channel in golang.org/x/crypto/ssh

[unknown] GO-2026-5932 — pkg:golang/golang.org/x/crypto@v0.54.0

The golang.org/x/crypto/openpgp package is unmaintained, unsafe by design, and has known security issues

[unknown] GO-2026-6094 — pkg:golang/github.com/google/cel-go@v0.29.2

JSON private fields exposed via NativeTypes and ParseStructTag in github.com/google/cel-go

Skipped or failed analyzers

bomdrift (fail): Error: parsing JSON in:

`/tmp/sba-analyze-1329137-1938-1788944924347275839-3/input.spdx` Caused by: expected value at line 1 column 1

inspektr_cli (fail): Error: Failed to scan for vulnerabilities Caused by: 0: SBOM format error: Failed to decode SBOM: expected value at line 1 column 1 1: Failed to decode SBOM: expected value at line 1 column 1

shieldbom (fail): Parsed 169 components from

`"/tmp/sba-analyze-1329137-1938-1788944924347275839-3/input.spdx"` (SPDX 2.3 (Tag-Value)) Found 0 vulnerabilities Found 20 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.