

ndaal SBOM Auditor — analysis of trivy_bom.json (SBOM #3)

SBOM metadata

Name: trivy_bom.json * Format: cyclonedx-json

Spec version: 1.6 * Components: 460 * Source: upload

SHA-256: c9f7545b5b67a708d9951870db5feab936948071abe999f5958c770ad154c47c

Ingested: 2026-08-24T14:26:22Z

Analyzer summary

syft 1.51.0 — ok — 0 finding(s)

grype 0.117.0 — ok — 2 finding(s)

trivy 0.74.0 — ok — 2 finding(s)

osv-scanner 2.5.1 — ok — 2 finding(s)

bomber 0.5.1 — ok — 3 finding(s)

bomdrift bomdrift 0.9.9 — ok — 12 finding(s)

inspektr_cli inspektr 0.1.9 — fail — 0 finding(s)

shieldbom shieldbom 0.3.0 — fail — 0 finding(s)

provenant provenant-cli 1.0.7 — ok — 0 finding(s)

Findings from grype

[high] GHSA-hfg8-hc9c-6c3h (CVE-2026-17106) — github.com/moby/go-archive@v0.2.1

moby/go-archive: Crafted tar archive can write outside the extraction directory

Fixed in: 0.3.0

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.55.0

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-2026-17106 — github.com/moby/go-archive@v0.2.1

moby/go-archive: Crafted tar archive can write outside the extraction directory

Fixed in: 0.3.0

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.55.0

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

Findings from osv-scanner

[unknown] GHSA-hfg8-hc9c-6c3h (CVE-2026-17106) — github.com/moby/go-archive@v0.2.1

moby/go-archive: Crafted tar archive can write outside the extraction directory

[unknown] GO-2026-5932 — golang.org/x/crypto@v0.55.0

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

Findings from bomber

[high] CVE-2026-17106 —

pkg:golang/github.com/moby/go-archive@v0.2.1?goarch=amd64&goos=linux&type=module

moby/go-archive: Crafted tar archive can write outside the extraction directory

[unknown] CVE-2026-33634 —

pkg:golang/github.com/aquasecurity/trivy@v0.74.0?goarch=amd64&goos=linux&type=module

Trivy ecosystem supply chain was briefly compromised in github.com/aquasecurity/trivy

[unknown] GO-2026-5932 —

pkg:golang/golang.org/x/crypto@v0.55.0?goarch=amd64&goos=linux&type=module

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

Findings from bomdrift

[high] bomdrift.cve —

pkg:golang/github.com/moby/go-archive@v0.2.1?goarch=amd64&goos=linux&type=module

GHSA-hfg8-hc9c-6c3h (HIGH) affects

pkg:golang/github.com/moby/go-archive@v0.2.1?goarch=amd64&goos=linux&type=module. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve —

pkg:golang/golang.org/x/crypto@v0.55.0?goarch=amd64&goos=linux&type=module

GO-2026-5932 (NONE) affects

pkg:golang/golang.org/x/crypto@v0.55.0?goarch=amd64&goos=linux&type=module. Review the advisory and update or pin a patched version.

[medium] bomdrift.typosquat —

pkg:golang/cel.dev/expr@v0.25.2?goarch=amd64&goos=linux&type=module

`cel.dev/expr` is similar to popular package `golang.org/x/exp` (similarity 0.94). Verify the package source before merging.

[medium] bomdrift.typosquat —

pkg:golang/github.com/aquasecurity/tml@v0.6.1?goarch=amd64&goos=linux&type=module

`github.com/aquasecurity/tml` is similar to popular package `github.com/burntsushi/toml` (similarity 0.92). Verify the package source before merging.

[medium] bomdrift.typosquat —

pkg:golang/github.com/go-logr/logr@v1.4.4?goarch=amd64&goos=linux&type=module

`github.com/go-logr/logr` is similar to popular package `github.com/sirupsen/logrus` (similarity 0.93). Verify the package source before merging.

[medium] bomdrift.typosquat —

pkg:golang/github.com/knqyf263/go-apk-version@v0.0.0-20200609155635-041fdbb8563f?goarch=

`github.com/knqyf263/go-apk-version` is similar to popular package `github.com/hashicorp/go-version` (similarity 0.93). Verify the package source before merging.

[medium] bomdrift.typosquat –

pkg:golang/github.com/moby/docker-image-spec@v1.3.1?goarch=amd64&goos=linux&type=module

`github.com/moby/docker-image-spec` is similar to popular package

`github.com/opencontainers/image-spec` (similarity 0.95). Verify the package source before merging.

[medium] bomdrift.typosquat –

pkg:golang/github.com/moby/moby/client@v0.5.1?goarch=amd64&goos=linux&type=module

`github.com/moby/moby/client` is similar to popular package `k8s.io/client-go` (similarity 0.93). Verify the package source before merging.

[medium] bomdrift.typosquat –

pkg:golang/go.opentelemetry.io/otel/exporters/otlp/otlptrace@v1.44.0?goarch=amd64&goos=linux

`go.opentelemetry.io/otel/exporters/otlp/otlptrace` is similar to popular package

`go.opentelemetry.io/otel/trace` (similarity 0.95). Verify the package source before merging.

[medium] bomdrift.typosquat –

pkg:golang/golang.org/x/xerrors@v0.0.0-20240903120638-7835f813f4da?goarch=amd64&goos=linux

`golang.org/x/xerrors` is similar to popular package `github.com/pkg/errors` (similarity 0.95). Verify the package source before merging.

[medium] bomdrift.typosquat –

pkg:golang/sigs.k8s.io/json@v0.0.0-20250730193827-2d320260d730?goarch=amd64&goos=linux

`sigs.k8s.io/json` is similar to popular package `github.com/tidwall/gjson` (similarity 0.93). Verify the package source before merging.

[medium] bomdrift.typosquat –

pkg:golang/sigs.k8s.io/kustomize/kyaml@v0.21.1?goarch=amd64&goos=linux&type=module

`sigs.k8s.io/kustomize/kyaml` is similar to popular package `sigs.k8s.io/yaml` (similarity 0.93). Verify the package source before merging.

Skipped or failed analyzers

inspektr_cli (fail): Error: Failed to scan for vulnerabilities Caused by: 0: SBOM format error: Failed to decode SBOM: invalid type: map, expected a sequence at line 10 column 6 1: Failed to decode SBOM: invalid type: map, expected a sequence at line 10 column 6

shieldbom (fail): Parsed 460 components from

"/tmp/sba-analyze-108681-3-1787581596783793061-1/input.cdx.json" (CycloneDX 1.5 (JSON)) Found 0 vulnerabilities Found 460 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.