

ndaal SBOM Auditor — analysis of demo-sbom.cdx.json (SBOM #2298)

SBOM metadata

Name: demo-sbom.cdx.json * Format: cyclonedx-json

Spec version: 1.6 * Components: 2 * Source: upload

SHA-256: 20c0635ac7bbc1658b9c2ca077f889099c1f940ee1a20f606b05b0541374c090

Ingested: 2026-09-20T19:32:02Z

Analyzer summary

syft 1.51.0 — ok — 0 finding(s)

grype 0.118.0 — ok — 13 finding(s)

trivy 0.74.0 — ok — 14 finding(s)

osv-scanner 2.5.1 — ok — 13 finding(s)

bomber 0.5.1 — ok — 13 finding(s)

bomdrift bomdrift 0.9.9 — ok — 14 finding(s)

inspektr_cli inspektr 0.1.9 — ok — 6 finding(s)

shieldbom shieldbom 0.3.0 — fail — 0 finding(s)

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

Findings from grype

[critical] GHSA-7rjr-3q55-vv33 (CVE-2021-45046) — log4j-core@2.14.1

Incomplete fix for Apache Log4j vulnerability

Fixed in: 2.16.0

[critical] GHSA-jfh8-c2jp-5v3q (CVE-2021-44228) — log4j-core@2.14.1

Remote code injection in Log4j

Fixed in: 2.15.0

[high] GHSA-35jh-r3h4-6jhm (CVE-2021-23337) — lodash@4.17.15

Command Injection in lodash

Fixed in: 4.17.21

[high] GHSA-p6mc-m468-83gw (CVE-2020-8203) — lodash@4.17.15

Prototype Pollution in lodash

Fixed in: 4.17.19

[high] GHSA-p6xc-xr62-6r2g (CVE-2021-45105) — log4j-core@2.14.1

Apache Log4j2 vulnerable to Improper Input Validation and Uncontrolled Recursion

Fixed in: 2.17.0

[high] GHSA-r5fr-rjxr-66jc (CVE-2026-4800) — lodash@4.17.15

lodash vulnerable to Code Injection via `\_.template` imports key names

Fixed in: 4.18.0

[medium] GHSA-29mw-wpgm-hmr9 (CVE-2020-28500) — lodash@4.17.15

Regular Expression Denial of Service (ReDoS) in lodash

Fixed in: 4.17.21

[medium] GHSA-3pxv-7cmr-fjr4 (CVE-2026-34480) — log4j-core@2.14.1

Apache Log4j Core: Silent log event loss in XmlLayout due to unescaped XML 1.0 forbidden characters

Fixed in: 2.25.4

[medium] GHSA-6hg6-v5c8-fphq (CVE-2026-34477) — log4j-core@2.14.1

Apache Log4j Core: `verifyHostName` attribute silently ignored in TLS configuration

Fixed in: 2.25.4

[medium] GHSA-8489-44mv-ggj8 (CVE-2021-44832) — log4j-core@2.14.1

Improper Input Validation and Injection in Apache Log4j2

Fixed in: 2.17.1

[medium] GHSA-f23m-r3pf-42rh (CVE-2026-2950) — lodash@4.17.15

lodash vulnerable to Prototype Pollution via array path bypass in `\_.unset` and `\_.omit`

Fixed in: 4.18.0

[medium] GHSA-vc5p-v9hr-52mj (CVE-2025-68161) — log4j-core@2.14.1

Apache Log4j does not verify the TLS hostname in its Socket Appender

Fixed in: 2.25.3

[medium] GHSA-xxjr-mmjv-4gpg (CVE-2025-13465) — lodash@4.17.15

Lodash has Prototype Pollution Vulnerability in `\_.unset` and `\_.omit` functions

Fixed in: 4.17.23

Findings from trivy

[critical] CVE-2021-44228 — org.apache.logging.log4j:log4j-core@2.14.1

log4j-core: Remote code execution in Log4j 2.x when logs contain an attacker-controlled string value

Fixed in: 2.15.0, 2.3.1, 2.12.2

[critical] CVE-2021-45046 — org.apache.logging.log4j:log4j-core@2.14.1

log4j-core: DoS in log4j 2.x with thread context message pattern and context lookup pattern (incomplete fix for CVE-2021-44228)

Fixed in: 2.16.0, 2.12.2

[high] CVE-2020-8203 — lodash@4.17.15

nodejs-lodash: prototype pollution in zipObjectDeep function

Fixed in: 4.17.19

[high] CVE-2021-23337 — lodash@4.17.15

nodejs-lodash: command injection via template

Fixed in: 4.17.21

[high] CVE-2021-45105 — org.apache.logging.log4j:log4j-core@2.14.1

log4j-core: DoS in log4j 2.x with Thread Context Map (MDC) input data contains a recursive lookup and

context lookup pattern

Fixed in: 2.12.3, 2.17.0, 2.3.1

[high] CVE-2026-4800 – lodash@4.17.15

lodash: lodash: Arbitrary code execution via untrusted input in template imports

Fixed in: 4.18.0

[high] NSWG-ECO-516 – lodash@4.17.15

Allocation of Resources Without Limits or Throttling

Fixed in: >=4.17.19

[medium] CVE-2020-28500 – lodash@4.17.15

nodejs-lodash: ReDoS via the toNumber, trim and trimEnd functions

Fixed in: 4.17.21

[medium] CVE-2021-44832 – org.apache.logging.log4j:log4j-core@2.14.1

log4j-core: remote code execution via JDBC Appender

Fixed in: 2.3.2, 2.12.4, 2.17.1

[medium] CVE-2025-13465 – lodash@4.17.15

lodash: prototype pollution in _.unset and _.omit functions

Fixed in: 4.17.23

[medium] CVE-2025-68161 – org.apache.logging.log4j:log4j-core@2.14.1

Apache Log4j: Apache Log4j Core: Information disclosure via missing TLS hostname verification

Fixed in: 2.25.3

[medium] CVE-2026-2950 – lodash@4.17.15

lodash: Lodash: Prototype pollution allows deletion of built-in prototype properties via array path bypass

Fixed in: 4.18.0

[medium] CVE-2026-34477 – org.apache.logging.log4j:log4j-core@2.14.1

org.apache.logging.log4j/log4j-core: Apache Log4j Core: Man-in-the-middle attack due to incomplete hostname verification

Fixed in: 2.25.4

[medium] CVE-2026-34480 – org.apache.logging.log4j:log4j-core@2.14.1

org.apache.logging.log4j/log4j-core: Apache Log4j Core: Invalid XML output causes denial of service in logging

Fixed in: 2.25.4

Findings from osv-scanner

[unknown] GHSA-29mw-wpgm-hmr9 (CVE-2020-28500) – lodash@4.17.15

Regular Expression Denial of Service (ReDoS) in lodash

[unknown] GHSA-35jh-r3h4-6jhm (CVE-2021-23337) – lodash@4.17.15

Command Injection in lodash

[unknown] GHSA-3pxv-7cmr-fjr4 (CVE-2026-34480) – log4j-core@2.14.1

Apache Log4j Core: Silent log event loss in XmlLayout due to unescaped XML 1.0 forbidden characters

[unknown] GHSA-6hg6-v5c8-fphq (CVE-2026-34477) — log4j-core@2.14.1

Apache Log4j Core: `verifyHostName` attribute silently ignored in TLS configuration

[unknown] GHSA-7rjr-3q55-vv33 (CVE-2021-45046) — log4j-core@2.14.1

Incomplete fix for Apache Log4j vulnerability

[unknown] GHSA-8489-44mv-ggj8 (CVE-2021-44832) — log4j-core@2.14.1

Improper Input Validation and Injection in Apache Log4j2

[unknown] GHSA-f23m-r3pf-42rh (CVE-2025-13465) — lodash@4.17.15

lodash vulnerable to Prototype Pollution via array path bypass in `\_.unset` and `\_.omit`

[unknown] GHSA-jfh8-c2jp-5v3q (CVE-2021-44228) — log4j-core@2.14.1

Remote code injection in Log4j

[unknown] GHSA-p6mc-m468-83gw (CVE-2020-8203) — lodash@4.17.15

Prototype Pollution in lodash

[unknown] GHSA-p6xc-xr62-6r2g (CVE-2021-45105) — log4j-core@2.14.1

Apache Log4j2 vulnerable to Improper Input Validation and Uncontrolled Recursion

[unknown] GHSA-r5fr-rjxr-66jc (CVE-2021-23337) — lodash@4.17.15

lodash vulnerable to Code Injection via `\_.template` imports key names

[unknown] GHSA-vc5p-v9hr-52mj (CVE-2025-68161) — log4j-core@2.14.1

Apache Log4j does not verify the TLS hostname in its Socket Appender

[unknown] GHSA-xxjr-mmjv-4gpg (CVE-2025-13465) — lodash@4.17.15

Lodash has Prototype Pollution Vulnerability in `\_.unset` and `\_.omit` functions

Findings from bomber

[critical] CVE-2021-44228 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Remote code injection in Log4j

[critical] CVE-2021-45046 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Incomplete fix for Apache Log4j vulnerability

[high] CVE-2020-8203 — pkg:npm/lodash@4.17.15

Prototype Pollution in lodash

[high] CVE-2021-23337 — pkg:npm/lodash@4.17.15

Command Injection in lodash

[high] CVE-2021-23337 — pkg:npm/lodash@4.17.15

lodash vulnerable to Code Injection via `\_.template` imports key names

[high] CVE-2021-45105 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Apache Log4j2 vulnerable to Improper Input Validation and Uncontrolled Recursion

[medium] CVE-2020-28500 — pkg:npm/lodash@4.17.15

Regular Expression Denial of Service (ReDoS) in lodash

[medium] CVE-2021-44832 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Improper Input Validation and Injection in Apache Log4j2

[medium] CVE-2025-13465 — pkg:npm/lodash@4.17.15

lodash vulnerable to Prototype Pollution via array path bypass in `_.unset` and _.omit``

[medium] CVE-2025-13465 — pkg:npm/lodash@4.17.15

Lodash has Prototype Pollution Vulnerability in `_.unset` and _.omit` functions`

[medium] CVE-2025-68161 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Apache Log4j does not verify the TLS hostname in its Socket Appender

[medium] CVE-2026-34477 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Apache Log4j Core: `verifyHostName` attribute silently ignored in TLS configuration`

[medium] CVE-2026-34480 — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

Apache Log4j Core: Silent log event loss in XmlLayout due to unescaped XML 1.0 forbidden characters

Findings from bomdrift

[high] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-7rjr-3q55-vv33 (CRITICAL) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[high] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-jfh8-c2jp-5v3q (CRITICAL) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[high] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-p6xc-xr62-6r2g (HIGH) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[high] bomdrift.cve — pkg:npm/lodash@4.17.15

GHSA-35jh-r3h4-6jhm (HIGH) affects pkg:npm/lodash@4.17.15. Review the advisory and update or pin a patched version.

[high] bomdrift.cve — pkg:npm/lodash@4.17.15

GHSA-p6mc-m468-83gw (HIGH) affects pkg:npm/lodash@4.17.15. Review the advisory and update or pin a patched version.

[high] bomdrift.cve — pkg:npm/lodash@4.17.15

GHSA-r5fr-rjxr-66jc (HIGH) affects pkg:npm/lodash@4.17.15. Review the advisory and update or pin a patched version.

[high] bomdrift.deprecated — pkg:npm/lodash@4.17.15

`lodash` is deprecated upstream: Bad release. Please use lodash@4.17.21` instead.`

[medium] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-3pxv-7cmr-fjr4 (MEDIUM) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-6hg6-v5c8-fphq (MEDIUM) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-8489-44mv-ggj8 (MEDIUM) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1

GHSA-vc5p-v9hr-52mj (MEDIUM) affects pkg:maven/org.apache.logging.log4j/log4j-core@2.14.1. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:npm/lodash@4.17.15

GHSA-29mw-wpgm-hmr9 (MEDIUM) affects pkg:npm/lodash@4.17.15. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:npm/lodash@4.17.15

GHSA-f23m-r3pf-42rh (MEDIUM) affects pkg:npm/lodash@4.17.15. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:npm/lodash@4.17.15

GHSA-xxjr-mmjv-4gpg (MEDIUM) affects pkg:npm/lodash@4.17.15. Review the advisory and update or pin a patched version.

Findings from inspektr_cli

[unknown] CVE-2020-28500 — pkg:npm/lodash@4.17.15

Regular Expression Denial of Service (ReDoS) in lodash
Fixed in: 4.17.21

[unknown] CVE-2020-8203 — pkg:npm/lodash@4.17.15

Prototype Pollution in lodash
Fixed in: 4.17.19

[unknown] CVE-2021-23337 — pkg:npm/lodash@4.17.15

Command Injection in lodash
Fixed in: 4.17.21

[unknown] CVE-2025-13465 — pkg:npm/lodash@4.17.15

lodash vulnerable to Prototype Pollution via array path bypass in `\_.unset` and `\_.omit`
Fixed in: 4.18.0

[unknown] CVE-2026-2950 — pkg:npm/lodash@4.17.15

Impact: Lodash versions 4.17.23 and earlier are vulnerable to prototype pollution in the `_.unset` and `_.omit` functions. The fix for (CVE-2025-13465: <https://github.com/lodash/lodash/security/advisories/GHSA-xxjr-mmjv-4gpg>) only guards against string key members, so an attacker can bypass the check by passing array-wrapped path segments. This allows deletion of properties from built-in prototypes such as `Object.prototype`, `Number.prototype`, and `String.prototype`. The issue permits deletion of prototype properties but does not allow overwriting their original behavior. Patches: This issue is patched in 4.18.0. Workarounds: None. Upgrade to the patched version.

Fixed in: 4.17.23

[unknown] CVE-2026-4800 — pkg:npm/lodash@4.17.15

Impact: The fix for CVE-2021-23337 (<https://github.com/advisories/GHSA-35jh-r3h4-6jhm>) added validation for the variable option in `_.template` but did not apply the same validation to `options.imports` key names. Both paths flow into the same `Function()` constructor sink. When an application passes untrusted input as `options.imports` key names, an attacker can inject default-parameter expressions that execute arbitrary code at template compilation time. Additionally, `_.template` uses `assignInWith` to merge imports, which enumerates inherited properties via `for..in`. If `Object.prototype` has been polluted by any other vector, the polluted keys are copied into the imports object and passed to `Function()`.

Patches: Users should upgrade to version 4.18.0. Workarounds: Do not pass untrusted input as key names in `options.imports`. Only use developer-controlled, static key names.

Fixed in: 4.18.0

Skipped or failed analyzers

shieldbom (fail): Parsed 2 components from

"/tmp/sba-analyze-2942566-2298-1789933292213505716-2/input.cdx.json" (CycloneDX 1.5 (JSON))

Found 0 vulnerabilities Found 2 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.