

ndaal SBOM Auditor — analysis of cdx_cdxgen_ansible-modules-extras.json (SBOM #4041)

SBOM metadata

Name: cdx_cdxgen_ansible-modules-extras.json * Format: cyclonedx-json

Spec version: 1.5 * Components: 3 * Source: upload

SHA-256: 9e3a0524bdf2b00ed672bdf63ba2473e5eec8dd288be3859ec94cd87eb27e6af

Ingested: 2026-10-05T09:20:34Z

Analyzer summary

syft 1.52.0 — ok — 0 finding(s)

grype 0.119.0 — fail — 0 finding(s)

trivy 0.74.0 — ok — 3 finding(s)

osv-scanner 2.6.0 — ok — 6 finding(s)

bomber 0.5.1 — ok — 6 finding(s)

bomdrift bomdrift 0.9.9 — ok — 6 finding(s)

inspektr_cli inspektr 0.1.9 — ok — 6 finding(s)

shieldbom shieldbom 0.3.0 — fail — 0 finding(s)

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

Findings from trivy

[medium] CVE-2024-56201 — jinja2@3.1.4

jinja2: Jinja has a sandbox breakout through malicious filenames

Fixed in: 3.1.5

[medium] CVE-2024-56326 — jinja2@3.1.4

jinja2: Jinja has a sandbox breakout through indirect reference to format method

Fixed in: 3.1.5

[medium] CVE-2025-27516 — jinja2@3.1.4

jinja2: Jinja sandbox breakout through attr filter selecting format method

Fixed in: 3.1.6

Findings from osv-scanner

[unknown] GHSA-cpwx-vrp4-4pq7 (CVE-2025-27516) — jinja2@3.1.4

Jinja2 vulnerable to sandbox breakout through attr filter selecting format method

[unknown] GHSA-gmj6-6f8f-6699 (CVE-2024-56201) — jinja2@3.1.4

Jinja has a sandbox breakout through malicious filenames

[unknown] GHSA-q2x7-8rv6-6q7h (CVE-2024-56326) — jinja2@3.1.4

Jinja has a sandbox breakout through indirect reference to format method

[unknown] PYSEC-2026-1471 (CVE-2025-27516) — jinja2@3.1.4

Jinja2 vulnerable to sandbox breakout through attr filter selecting format method

[unknown] PYSEC-2026-1472 (CVE-2024-56201) — jinja2@3.1.4

Jinja has a sandbox breakout through malicious filenames

[unknown] PYSEC-2026-1475 (CVE-2024-56326) — jinja2@3.1.4

Jinja has a sandbox breakout through indirect reference to format method

Findings from bomber

[medium] CVE-2024-56201 — pkg:pypi/jinja2@3.1.4

Jinja has a sandbox breakout through malicious filenames

[medium] CVE-2024-56326 — pkg:pypi/jinja2@3.1.4

Jinja has a sandbox breakout through indirect reference to format method

[medium] CVE-2025-27516 — pkg:pypi/jinja2@3.1.4

Jinja2 vulnerable to sandbox breakout through attr filter selecting format method

[unknown] CVE-2024-56201 — pkg:pypi/jinja2@3.1.4

Jinja has a sandbox breakout through malicious filenames

[unknown] CVE-2024-56326 — pkg:pypi/jinja2@3.1.4

Jinja has a sandbox breakout through indirect reference to format method

[unknown] CVE-2025-27516 — pkg:pypi/jinja2@3.1.4

Jinja2 vulnerable to sandbox breakout through attr filter selecting format method

Findings from bomdrift

[medium] bomdrift.cve — pkg:pypi/jinja2@3.1.4

GHSA-cpwx-vrp4-4pq7 (MEDIUM) affects pkg:pypi/jinja2@3.1.4. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:pypi/jinja2@3.1.4

GHSA-gmj6-6f8f-6699 (MEDIUM) affects pkg:pypi/jinja2@3.1.4. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:pypi/jinja2@3.1.4

GHSA-q2x7-8rv6-6q7h (MEDIUM) affects pkg:pypi/jinja2@3.1.4. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:pypi/jinja2@3.1.4

PYSEC-2026-1471 (NONE) affects pkg:pypi/jinja2@3.1.4. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:pypi/jinja2@3.1.4

PYSEC-2026-1472 (NONE) affects pkg:pypi/jinja2@3.1.4. Review the advisory and update or pin a patched version.

[medium] bomdrift.cve — pkg:pypi/jinja2@3.1.4

PYSEC-2026-1475 (NONE) affects pkg:pypi/jinja2@3.1.4. Review the advisory and update or pin a patched version.

Findings from inspektr_cli

[unknown] CVE-2014-0012 — pkg:pypi/jinja2@3.1.4

FileSystemBytecodeCache in Jinja2 2.7.2 does not properly create temporary directories, which allows local users to gain privileges by pre-creating a temporary directory with a user's uid. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-1402.

[unknown] CVE-2014-1402 — pkg:pypi/jinja2@3.1.4

The default configuration for bccache.FileSystemBytecodeCache in Jinja2 before 2.7.2 does not properly create temporary files, which allows local users to gain privileges via a crafted .cache file with a name starting with __jinja2_ in /tmp.

[unknown] CVE-2019-8341 — pkg:pypi/jinja2@3.1.4

An issue was discovered in Jinja2 2.10. The from_string function is prone to Server Side Template Injection (SSTI) where it takes the "source" parameter as a template object, renders it, and then returns it. The attacker can exploit it with {{INJECTION COMMANDS}} in a URI. NOTE: The maintainer and multiple third parties believe that this vulnerability isn't valid because users shouldn't use untrusted templates without sandboxing

[unknown] CVE-2024-56201 — pkg:pypi/jinja2@3.1.4

Jinja has a sandbox breakout through malicious filenames

Fixed in: 3.1.5

[unknown] CVE-2024-56326 — pkg:pypi/jinja2@3.1.4

Jinja has a sandbox breakout through indirect reference to format method

Fixed in: 3.1.5

[unknown] CVE-2025-27516 — pkg:pypi/jinja2@3.1.4

Jinja2 vulnerable to sandbox breakout through attr filter selecting format method

Fixed in: 3.1.6

Skipped or failed analyzers

grype (fail): failed to produce parseable output

shieldbom (fail): Parsed 3 components from

"/tmp/sba-analyze-10477-4041-1791192081723411086-35/input.cdx.json" (CycloneDX 1.5 (JSON))

Found 0 vulnerabilities Found 3 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.