CMU penrose

Created by Scott A Hissam, last updated 5 minutes ago • 12 minute read

> **WARNING: Do not hand edit, this page is subject to automatic updates.**

- Critical and High vulnerabilities
- Critical and High maliciousCodeRisk
- Critical and High engineeringRisk
- Critical and High authorsRisk
- Critical, High, Medium, and Low licenseRisk

<table>
<tr><th>OSS Project Report</th><th>Response</th></tr>
<tr><td>Overview</td><td></td></tr>
<tr><td>Background</td><td>penrose/penrose, Create beautiful diagrams just by typing notation in plain text.</td></tr>
<tr><td>Application or Library</td><td>Manual (ask)</td></tr>
<tr><td>Current as of</td><td>Date: 08-12-2025 (project queried 0 days ago)</td></tr>
<tr><td>OSS-P4/R Outlook</td><td>
<table>
<tr><td>Overall</td><td>Project (5.9)</td><td>Product (6.7)</td><td>Protection (6.1)</td><td>Policy (7.1)</td></tr>
<tr><td>MY Checks</td><td>Project (10.0)</td><td></td><td></td><td>Policy (10.0)</td></tr>
<tr><td>OSSF Scorecard</td><td>Project (3.2)</td><td>Product (5.0)</td><td>Protection (6.1)</td><td>Policy (3.3)</td></tr>
<tr><td>MITRE Hipcheck</td><td>Project (4.4)</td><td>Product (8.3)</td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>DOD CIO Criteria</td><td>
<table>
<tr><td>Criteria</td><td>Security (6.6)</td><td>Integrity (0.8)</td><td>Dependencies (6.0)</td><td>Malicious Actors (10.0)</td><td>Long-Term Support (7.6)</td><td>Suitability (10.0)</td></tr>
<tr><td>MY Checks</td><td></td><td></td><td></td><td></td><td>Long-Term Support (10.0)</td><td>Suitability (10.0)</td></tr>
<tr><td>OSSF Scorecard</td><td>Security (4.9)</td><td>Integrity (1.6)</td><td>Dependencies (6.0)</td><td></td><td>Long-Term Support (4.0)</td><td>Suitability (10.0)</td></tr>
<tr><td>MITRE Hipcheck</td><td>Security (8.3)</td><td>Integrity (0.0)</td><td></td><td>Malicious Actors (10.0)</td><td>Long-Term Support (8.9)</td><td></td></tr>
</table>
</td></tr>
<tr><td>Summarized Scores By CIO Criteria</td><td>
<table>
<tr><td>Criteria:</td><td>Security</td><td>Integrity</td><td>Dependencies</td><td>Malicious Actors</td><td>Long-Term Support</td><td>Suitability</td></tr>
<tr><td>MY Checks:</td><td></td><td></td><td></td><td></td><td>Project Forked(false/false)
Problem Reporting(true/true)
Project Abandoned(false/false)
Dependent Projects Abandoned(0/0)</td><td>Restrictive License(s)(0/0)</td></tr>
<tr><td>OSSF Scorecard: (higher's better) 4.3/10.0</td><td>Binary Artifacts(10/3.3)
❌Branch Protection(3/3.3)
Dangerous Workflow(10/3.3)
❌Token Permissions(0/3.3)
❌Vulnerabilities(0/3.3)
⚠Webhooks(NaN/3.3)</td><td>❌Code Review(1/3.3)
CI Tests(10/3.3)
❌Fuzzing(0/3.3)
❌SAST(0/3.3)
⚠ Packaging(NaN/3.3)
⚠Signed Releases(NaN/3.3)</td><td>Dependency Update Tool(10/3.3)
❌Pinned Dependencies(0/3.3)</td><td></td><td>Contributors(10/3.3)
Maintained(6/3.3)
❌CII Best Practices(0/3.3)
❌Security Policy(0/3.3)</td><td>License(10/3.3)</td></tr>
<tr><td>MITRE Hipcheck: (score ≤ threshold) ❌ INVESTIGATE risk rated as 0.55, acceptable below or equal to 0.50</td><td>Binary Artifacts(0.0/0)
Large Commits(0.01/0.02)
Malware Entropy(0.0/0)
⚠ Typosquatting(NaN/true)</td><td>❌Self Reviews(0.6/0.2)
❌Fuzz Testing(false/true)
❌Pull Reviews(0.6/0.05)</td><td></td><td>Author Affiliation(0.0/0)</td><td>Commit Activity(8.0/71)</td><td></td></tr>
</table>
</td></tr>
<tr><td>Security</td><td></td></tr>
<tr><td>Trusted Source(s)</td><td>Source: https://github.com/penrose/penrose
D-U-N-S Availability: Manual
Repo or Mirror: Manual</td></tr>
<tr><td>Public or Private</td><td>Visibility is: public
Private is: false</td></tr>
<tr><td>Fully Unrestricted</td><td>Read-Only: manual
Write: manual</td></tr>
<tr><td>Login Credentials</td><td>Manual</td></tr>
<tr><td>Use of Repository Protections</td><td>❌3/10 as branch protection is not maximal on development and all release branches
10/10 as no dangerous workflow patterns detected
❌0/10 as detected GitHub workflow tokens with excessive permissions, and
⚠ check that webhooks is configured supporting secrets not run</td></tr>
<tr><td>Large Commits</td><td>Detected some unusually large commits being 0.01 found under or at the 0.02 permitted threshold (Churn)</td></tr>
<tr><td>Obfuscated Code</td><td>Detected no unusual-looking commits being 0.0 found under or at the 0 permitted threshold (Entropy)</td></tr>
<tr><td>Binary Artifact(s)</td><td>10/10 as no binaries found in the repo with binaries potentially containing code being 0 found under or at the 0 permitted threshold</td></tr>
<tr><td>Typosquatting Risk</td><td>⚠Failed to analyze for typos - can't identify a known language</td></tr>
<tr><td>Known Vulnerabilities</td><td>❌0/10 as 43 existing vulnerabilities detected (open, known unfixed vulnerabilities).
Other detected vuls including other dependencies identified potentially: 8 critical; 38 high; 69 medium; 7 low
criticals: ❌2 GHSA-9crc-q9x8-hgqq; 3 GHSA-fjxv-7rqg-78g4; 1 GHSA-j9fq-vwqv-2fm2; 2 GHSA-jf85-cpcp-j695</td></tr>
<tr><td>Integrity</td><td></td></tr>
<tr><td>Peer Reviews</td><td>Count pending; and activity is ❌1/10 as Found 2/17 approved changesets -- score normalized to 1 with change requests often lacking approving review prior to merge with 58.241% ❌over the 5.0% threshold and commits too often applied by the author with 62.83% ❌over the 20.0% threshold</td></tr>
<tr><td>Use of Code and Security Scanners</td><td>❌0/10 as project is not fuzzed with repository ❌not receiving regular fuzz testing
❌0/10 as SAST tool is not run on all commits -- score normalized to 0, and
10/10 as 30 out of 30 merged PRs checked by a CI test -- score normalized to 10</td></tr>
<tr><td>Signed Commits</td><td>Manual</td></tr>
</table>

Cryptographically Signed Commits	100 of the last 100 commits have a valid cryptographic signature.
Cryptographically Signed Releases & Artifacts	⚠-1/10 as no releases found, and ⚠-1/10 as packaging workflow not detected; investigate if any such signing(s) are crytopgraphic
Dependencies	
Published Software Bill of Materials	SPDX-2.3,Tool: protobom-v0.0.0-20250805170613-cf5b071169fb+dirty,Tool: GitHub.com-Dependency-Graph Language package managers detected: 2499 npm, 1156 cargo, 1138 github, 549 githubactions, 11 gem, 9 pypi, 1 golang
Dependencies Pinned to Version	❌0/10 as dependency not pinned by hash detected -- score normalized to 0
Dependencies Up to Date	Yes with update tool detected; investigate if any dependencies apply to more than the pipeline
Number OSS Dependencies	Primary: Total found: 2508, dependencies pulled: 2507, dependencies unknown: ⚠1 Secondary: Total found: 2855, dependencies pulled: ⚠0, dependencies unknown: ⚠2855 Tertiary and greater (Max search depth realized 2): Total found: ⚠0, dependencies pulled: ⚠0, dependencies unknown: 0
Number Proprietary Dependencies	Primary: Manual Secondary and tertiary: Manual
Malicious Actors	
Author(s) Known to Commit Vulnerabilities	Manual
Author(s) Known to Commit Malicious Code	Hipcheck contributors affiliations being 0 found at or under the 0 permitted threshold
Long Term Support	
Project Summary	penrose/penrose, Create beautiful diagrams just by typing notation in plain text.
Individual or Organization	Organization Details: Name: Penrose Company: Not Reported Bio: Create beautiful diagrams just by typing mathematical notation in plain text. Email: team@penrose.ink Blog: https://penrose.cs.cmu.edu/ Geo: Carnegie Mellon University Source: GitHub
Organization Type	Pending, see: https://api.github.com/users/penrose/orgs logistics database D-U-N-S code: Manual
SLSA Level	Pending: (ask)
Best Practices	❌0/10 as no effort to earn an OpenSSF best practices badge detected
Number of Abandoned Project(s)	penrose is not archived; 0 of the primary dependencies are abandoned; ⚠tertiary (other) dependencies are not checked at this time
OSSF's Activity (criticality) Score (work in progress)	0.43/1.0 (higher's better)
Commits	Days since last commit: 1 days, on Mon Aug 11 16:24:34 UTC 2025, reported 0 days ago Days since first commit: 3246 days, on Thu Sep 22 04:47:19 UTC 2016, reported 0 days ago Activity: 6/10 with 6 commit(s) and 2 issue activity found in the last 90 days -- score normalized to 6 with most recent activity being 8 weeks under or at the 71 week threshold
Number of Contributors	Core: Count pending Other: 37 Organizational diversity: 10/10 as project has 7 contributing companies or organizations
Problem Reporting Process	Yes with 182 open issues
Vulnerability Reporting Process	❌0/10 as security policy file not detected
Suitability	
License	License: MIT License SPDX_ID: MIT
License Risk	No restrictive license detected Detected no product or dependent license(s) detected and no impacts potentially reported from dependencies
About this report	
Created	Tue Aug 12 21:32:16 UTC 2025
Version	pubRel 250516evie (branch: publicRelease)
Analysis Source	Package SBOM: penrose_ghapi_sbom.json, 742799016758a9b3cad4ee084eadfa9a
Analysis ID	SBOM created on 2025-08-12T18:54:09Z (complete)
Runtime	Approximately 158 minute(s) (this run), for a total of 158 minute(s) over 1 run(s)
Command line	/home/hc_user/.local/bin/scir-oss.sh -l -v -C penrose -G penrose/penrose -P github:sbom
Dependency and Scoring depth	2, 0
Comment/Caveats	I: config image _OSSFSC=/home/hc_user/.local/bin/scorecard I: config image _MITRHC=/home/hc_user/.local/bin/hc I: config setting _OSSSCIRsettings=/home/hc_user/.local/bin/settings I: config setting _MITRHCconfig=/home/hc_user/.local/bin/settings/hipcheck/config I: config setting _MITRHCscripts=/home/hc_user/.local/bin/settings/hipcheck/scripts I: config setting _OSSSCIRlicenseDB=/home/hc_user/.local/bin/settings/mychecks/licenseDB.json I: config setting _OSSSCIRrepoResolveDB= I: env setting _TERTIARY_BLACKLIST='pkg:npm|^npm:' W: could not determine OSSF/criticality_score version I: CA Certificate Trust Store () I: SBOM dependencies in 'github' are declared to include transitive dependencies - issue depth is 0 (change with -i) W: coalesce_scorecards: counted 1221 missing project scorecard(s) I: Thresholds for OSSF Scorecard scores set at 3.3 I: Threshold for OSSF Criticality Score set at 0.2 I: Local cache tolerance set to 2 days I: Days active tolerance set to 497 days I: Days for a new project set to 245 days I: Contributors tolerance set to 3 ids W: Some responses may require manual investigation if necessary (look for 'manual')
Powered by	OSSF/Scorecard v5.2.1, OSSF/Critical Score unknown, MITRE Hipcheck 3.4.0, grype 0.93.0 db v6.0.2 built on 2025-06-05T04:11:46Z

footnotes	**Data in this report is from public sources and with some being self-reported (e.g., emails, country of origin, names)**. **Pending/manual**: *Check requires manual intervention.* **Restrictive license**: *A license that requires code changes be openly published (i.e., copyleft).* ⚠️**-1/n**: *Score could not be valued due to source data.* ⚠️**NaN**: *Score could not be computed due to source data.* ⚠️**n**: *Score indicated a possible risk which requires investigation.* ⚠️ **not checked**: *Check is coming soon.* ❌**m/n**: *Score did not meet goals and/or thresholds.* ❌**n**: *Score did not meet goals and/or thresholds.* ❌**Yes/No**: *Score did not meet goals and/or thresholds.* ❌**true/false**: *Score did not meet goals and/or thresholds.*

Critical and High vulnerabilities

Package	Impact	Description
pkg:npm/vitest@%5E0.31 version <=0.0.125 (unknown)	CV-GHSA-9crc-q9x8-hgqq	**Overview** Vitest allows Remote Code Execution when accessing a malicious website while Vitest API server is listening **Grype Data Source**: https://github.com/advisories/GHSA-9crc-q9x8-hgqq **Recommendation** Fix available in None Provided **References** https://github.com/vitest-dev/vitest/blob/9a581e1c43e5c02b11e2a8026a55ce6a8cb35114/packages/vitest/src/api/setup.ts#L32-L46 https://github.com/vitest-dev/vitest/blob/9a581e1c43e5c02b11e2a8026a55ce6a8cb35114/packages/vitest/src/api/setup.ts#L66-L76 https://github.com/vitest-dev/vitest/security/advisories/GHSA-9crc-q9x8-hgqq https://vitest.dev/config/#api **CVE:** CVE-2025-24964 - **CVSS**: 9.6
pkg:npm/vitest@%5E0.31.1 version <=0.0.125 (unknown)	CV-GHSA-9crc-q9x8-hgqq	**Overview** Vitest allows Remote Code Execution when accessing a malicious website while Vitest API server is listening **Grype Data Source**: https://github.com/advisories/GHSA-9crc-q9x8-hgqq **Recommendation** Fix available in None Provided **References** https://github.com/vitest-dev/vitest/blob/9a581e1c43e5c02b11e2a8026a55ce6a8cb35114/packages/vitest/src/api/setup.ts#L32-L46 https://github.com/vitest-dev/vitest/blob/9a581e1c43e5c02b11e2a8026a55ce6a8cb35114/packages/vitest/src/api/setup.ts#L66-L76 https://github.com/vitest-dev/vitest/security/advisories/GHSA-9crc-q9x8-hgqq https://vitest.dev/config/#api **CVE:** CVE-2025-24964 - **CVSS**: 9.6
pkg:npm/form-data@2.3.3 version <2.5.4 (unknown)	CV-GHSA-fjxv-7rqg-78g4	**Overview** form-data uses unsafe random function in form-data for choosing boundary **Grype Data Source**: https://github.com/advisories/GHSA-fjxv-7rqg-78g4 **Recommendation** Fix available in 2.5.4 **References** https://github.com/form-data/form-data/commit/3d1723080e6577a66f17f163ecd345a21d8d0fd0 https://github.com/form-data/form-data/security/advisories/GHSA-fjxv-7rqg-78g4 https://github.com/form-data/form-data/security/advisories/GHSA-fjxv-7rqg-78g4 **CVE:** CVE-2025-7783 - **CVSS**: null
pkg:npm/form-data@2.5.1 version <2.5.4 (unknown)	CV-GHSA-fjxv-7rqg-78g4	**Overview** form-data uses unsafe random function in form-data for choosing boundary **Grype Data Source**: https://github.com/advisories/GHSA-fjxv-7rqg-78g4 **Recommendation** Fix available in 2.5.4 **References** https://github.com/form-data/form-data/commit/3d1723080e6577a66f17f163ecd345a21d8d0fd0 https://github.com/form-data/form-data/security/advisories/GHSA-fjxv-7rqg-78g4 https://github.com/form-data/form-data/security/advisories/GHSA-fjxv-7rqg-78g4 **CVE:** CVE-2025-7783 - **CVSS**: null
pkg:npm/form-data@4.0.0 version >=4.0.0, <4.0.4 (unknown)	CV-GHSA-fjxv-7rqg-78g4	**Overview** form-data uses unsafe random function in form-data for choosing boundary **Grype Data Source**: https://github.com/advisories/GHSA-fjxv-7rqg-78g4 **Recommendation** Fix available in 4.0.4 **References** https://github.com/form-data/form-data/commit/3d1723080e6577a66f17f163ecd345a21d8d0fd0 https://github.com/form-data/form-data/security/advisories/GHSA-fjxv-7rqg-78g4 https://github.com/form-data/form-data/security/advisories/GHSA-fjxv-7rqg-78g4 **CVE:** CVE-2025-7783 - **CVSS**: null
pkg:npm/parse-url@6.0.2 version <8.1.0 (unknown)	CV-GHSA-j9fq-vwqv-2fm2	**Overview** Server-Side Request Forgery (SSRF) in GitHub repository ionicabizau/parse-url **Grype Data Source**: https://github.com/advisories/GHSA-j9fq-vwqv-2fm2 **Recommendation** Fix available in 8.1.0 **References** https://github.com/ionicabizau/parse-url/commit/b88c81df8f4c5168af454eaa4f92afa9349e4e13 https://huntr.dev/bounties/1b4c972a-abc8-41eb-a2e1-696db746b5fd https://github.com/ionicabizau/parse-url/commit/b88c81df8f4c5168af454eaa4f92afa9349e4e13 https://huntr.dev/bounties/1b4c972a-abc8-41eb-a2e1-696db746b5fd **CVE:** CVE-2022-2900 - **CVSS**: 9.1

pkg:npm/lodash@%5E4.17.15 version <4.17.12 (unknown)	CV-GHSA-jf85-cpcp-j695	**Overview** Prototype Pollution in lodash **Grype Data Source**: https://github.com/advisories/GHSA-jf85-cpcp-j695 **Recommendation** Fix available in 4.17.12 **References** https://access.redhat.com/errata/RHSA-2019:3024 https://security.netapp.com/advisory/ntap-20191004-0005/ https://snyk.io/vuln/SNYK-JS-LODASH-450202 https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpuoct2020.html https://access.redhat.com/errata/RHSA-2019:3024 https://security.netapp.com/advisory/ntap-20191004-0005/ https://snyk.io/vuln/SNYK-JS-LODASH-450202 https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpuoct2020.html **CVE:** CVE-2019-10744 - **CVSS**: 9.1
pkg:npm/lodash@%5E4.17.21 version <4.17.12 (unknown)	CV-GHSA-jf85-cpcp-j695	**Overview** Prototype Pollution in lodash **Grype Data Source**: https://github.com/advisories/GHSA-jf85-cpcp-j695 **Recommendation** Fix available in 4.17.12 **References** https://access.redhat.com/errata/RHSA-2019:3024 https://security.netapp.com/advisory/ntap-20191004-0005/ https://snyk.io/vuln/SNYK-JS-LODASH-450202 https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpuoct2020.html https://access.redhat.com/errata/RHSA-2019:3024 https://security.netapp.com/advisory/ntap-20191004-0005/ https://snyk.io/vuln/SNYK-JS-LODASH-450202 https://support.f5.com/csp/article/K47105354?utm_source=f5support&amp%3Butm_medium=RSS https://www.oracle.com/security-alerts/cpujan2021.html https://www.oracle.com/security-alerts/cpuoct2020.html **CVE:** CVE-2019-10744 - **CVSS**: 9.1
pkg:npm/ip@1.1.5 version <=2.0.1 (unknown)	HV-GHSA-2p57-rm9w-gvfp	**Overview** ip SSRF improper categorization in isPublic **Grype Data Source**: https://github.com/advisories/GHSA-2p57-rm9w-gvfp **Recommendation** Fix available in None Provided **References** https://github.com/indutny/node-ip/issues/150 https://github.com/indutny/node-ip/pull/143 https://github.com/indutny/node-ip/pull/144 https://github.com/indutny/node-ip/issues/150 https://github.com/indutny/node-ip/pull/143 https://github.com/indutny/node-ip/pull/144 https://security.netapp.com/advisory/ntap-20250117-0010/ **CVE:** CVE-2024-29415 - **CVSS**: 8.1
pkg:npm/vite@%5E4 version <2.9.16 (unknown)	HV-GHSA-353f-5xf4-qw67	**Overview** Vite Server Options (server.fs.deny) can be bypassed using double forward-slash (//) **Grype Data Source**: https://github.com/advisories/GHSA-353f-5xf4-qw67 **Recommendation** Fix available in 2.9.16 **References** https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32 https://github.com/vitejs/vite/pull/13348 https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67 https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32 https://github.com/vitejs/vite/pull/13348 https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67 **CVE:** CVE-2023-34092 - **CVSS**: 7.5
pkg:npm/vite@%5E4.0.4 version <2.9.16 (unknown)	HV-GHSA-353f-5xf4-qw67	**Overview** Vite Server Options (server.fs.deny) can be bypassed using double forward-slash (//) **Grype Data Source**: https://github.com/advisories/GHSA-353f-5xf4-qw67 **Recommendation** Fix available in 2.9.16 **References** https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32 https://github.com/vitejs/vite/pull/13348 https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67 https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32 https://github.com/vitejs/vite/pull/13348 https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67 **CVE:** CVE-2023-34092 - **CVSS**: 7.5
pkg:npm/vite@%5E5.2.1 version <2.9.16 (unknown)	HV-GHSA-353f-5xf4-qw67	**Overview** Vite Server Options (server.fs.deny) can be bypassed using double forward-slash (//) **Grype Data Source**: https://github.com/advisories/GHSA-353f-5xf4-qw67 **Recommendation** Fix available in 2.9.16 **References** https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32 https://github.com/vitejs/vite/pull/13348 https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67 https://github.com/vitejs/vite/commit/813ddd6155c3d54801e264ba832d8347f6f66b32 https://github.com/vitejs/vite/pull/13348 https://github.com/vitejs/vite/security/advisories/GHSA-353f-5xf4-qw67

		CVE: CVE-2023-34092 - **CVSS**: 7.5
pkg:npm/lodash.template@4.5.0 version <=4.5.0 (unknown)	HV-GHSA-35jh-r3h4-6jhm	**Overview** Command Injection in lodash **Grype Data Source**: https://github.com/advisories/GHSA-35jh-r3h4-6jhm **Recommendation** Fix available in None Provided **References** https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851 https://security.netapp.com/advisory/ntap-20210312-0006/ https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929 https://snyk.io/vuln/SNYK-JS-LODASH-1040724 https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2021.html https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851 https://security.netapp.com/advisory/ntap-20210312-0006/ https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929 https://snyk.io/vuln/SNYK-JS-LODASH-1040724 https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2021.html **CVE:** CVE-2021-23337 - **CVSS**: 7.2
pkg:npm/lodash@%5E4.17.15 version <4.17.21 (unknown)	HV-GHSA-35jh-r3h4-6jhm	**Overview** Command Injection in lodash **Grype Data Source**: https://github.com/advisories/GHSA-35jh-r3h4-6jhm **Recommendation** Fix available in 4.17.21 **References** https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851 https://security.netapp.com/advisory/ntap-20210312-0006/ https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929 https://snyk.io/vuln/SNYK-JS-LODASH-1040724 https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2021.html https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851 https://security.netapp.com/advisory/ntap-20210312-0006/ https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929 https://snyk.io/vuln/SNYK-JS-LODASH-1040724 https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2021.html **CVE:** CVE-2021-23337 - **CVSS**: 7.2
pkg:npm/lodash@%5E4.17.21 version <4.17.21 (unknown)	HV-GHSA-35jh-r3h4-6jhm	**Overview** Command Injection in lodash **Grype Data Source**: https://github.com/advisories/GHSA-35jh-r3h4-6jhm **Recommendation** Fix available in 4.17.21 **References** https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851 https://security.netapp.com/advisory/ntap-20210312-0006/ https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929 https://snyk.io/vuln/SNYK-JS-LODASH-1040724 https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2021.html https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/lodash/lodash/blob/ddfd9b11a0126db2302cb70ec9973b66baec0975/lodash.js%23L14851 https://security.netapp.com/advisory/ntap-20210312-0006/ https://snyk.io/vuln/SNYK-JAVA-ORGFUJIONWEBJARS-1074932 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1074930 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWER-1074928 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSBOWERGITHUBLODASH-1074931 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1074929 https://snyk.io/vuln/SNYK-JS-LODASH-1040724 https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpujul2022.html https://www.oracle.com/security-alerts/cpuoct2021.html **CVE:** CVE-2021-23337 - **CVSS**: 7.2
pkg:npm/parse-path@4.0.4 version <5.0.0 (unknown)	HV-GHSA-3j8f-xvm3-ffx4	**Overview** Authorization Bypass in parse-path

		Grype Data Source: https://github.com/advisories/GHSA-3j8f-xvm3-ffx4 **Recommendation** Fix available in 5.0.0 **References** https://github.com/ionicabizau/parse-path/commit/f9ad8856a3c8ae18e1cf4caef5edbabbc42840e8 https://huntr.dev/bounties/afffb2bd-fb06-4144-829e-ecbbcbc85388 https://github.com/ionicabizau/parse-path/commit/f9ad8856a3c8ae18e1cf4caef5edbabbc42840e8 https://huntr.dev/bounties/afffb2bd-fb06-4144-829e-ecbbcbc85388 **CVE:** CVE-2022-0624 - **CVSS**: 7.3
pkg:npm/solid-js@%5E1 version <1.9.4 (unknown)	HV-GHSA-3qxh-p7jc-5xh6	**Overview** Solid Lacks Escaping of HTML in JSX Fragments allows for Cross-Site Scripting (XSS) **Grype Data Source**: https://github.com/advisories/GHSA-3qxh-p7jc-5xh6 **Recommendation** Fix available in 1.9.4 **References** https://github.com/solidjs/solid/commit/b93956f28ed75469af6976a98728e313d0edd236 https://github.com/solidjs/solid/security/advisories/GHSA-3qxh-p7jc-5xh6 https://github.com/solidjs/solid/security/advisories/GHSA-3qxh-p7jc-5xh6 **CVE:** CVE-2025-27109 - **CVSS**: 7.3
pkg:npm/solid-js@1.7.5 version <1.9.4 (unknown)	HV-GHSA-3qxh-p7jc-5xh6	**Overview** Solid Lacks Escaping of HTML in JSX Fragments allows for Cross-Site Scripting (XSS) **Grype Data Source**: https://github.com/advisories/GHSA-3qxh-p7jc-5xh6 **Recommendation** Fix available in 1.9.4 **References** https://github.com/solidjs/solid/commit/b93956f28ed75469af6976a98728e313d0edd236 https://github.com/solidjs/solid/security/advisories/GHSA-3qxh-p7jc-5xh6 https://github.com/solidjs/solid/security/advisories/GHSA-3qxh-p7jc-5xh6 **CVE:** CVE-2025-27109 - **CVSS**: 7.3
pkg:npm/cross-spawn@6.0.5 version <6.0.6 (unknown)	HV-GHSA-3xgq-45jj-v275	**Overview** Regular Expression Denial of Service (ReDoS) in cross-spawn **Grype Data Source**: https://github.com/advisories/GHSA-3xgq-45jj-v275 **Recommendation** Fix available in 6.0.6 **References** https://github.com/moxystudio/node-cross-spawn/commit/5ff3a07d9add449021d806e45c4168203aa833ff https://github.com/moxystudio/node-cross-spawn/commit/640d391fde65388548601d95abedccc12943374f https://github.com/moxystudio/node-cross-spawn/pull/160 https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-8366349 https://security.snyk.io/vuln/SNYK-JS-CROSSSPAWN-8303230 **CVE:** CVE-2024-21538 - **CVSS**: 7.5
pkg:npm/cross-spawn@7.0.3 version >=7.0.0, <7.0.5 (unknown)	HV-GHSA-3xgq-45jj-v275	**Overview** Regular Expression Denial of Service (ReDoS) in cross-spawn **Grype Data Source**: https://github.com/advisories/GHSA-3xgq-45jj-v275 **Recommendation** Fix available in 7.0.5 **References** https://github.com/moxystudio/node-cross-spawn/commit/5ff3a07d9add449021d806e45c4168203aa833ff https://github.com/moxystudio/node-cross-spawn/commit/640d391fde65388548601d95abedccc12943374f https://github.com/moxystudio/node-cross-spawn/pull/160 https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-8366349 https://security.snyk.io/vuln/SNYK-JS-CROSSSPAWN-8303230 **CVE:** CVE-2024-21538 - **CVSS**: 7.5
pkg:npm/lodash@%5E4.17.15 version <4.17.11 (unknown)	HV-GHSA-4xc9-xhrj-v574	**Overview** Prototype Pollution in lodash **Grype Data Source**: https://github.com/advisories/GHSA-4xc9-xhrj-v574 **Recommendation** Fix available in 4.17.11 **References** https://hackerone.com/reports/380873 https://security.netapp.com/advisory/ntap-20190919-0004/ https://hackerone.com/reports/380873 https://security.netapp.com/advisory/ntap-20190919-0004/ **CVE:** CVE-2018-16487 - **CVSS**: null
pkg:npm/lodash@%5E4.17.21 version <4.17.11 (unknown)	HV-GHSA-4xc9-xhrj-v574	**Overview** Prototype Pollution in lodash **Grype Data Source**: https://github.com/advisories/GHSA-4xc9-xhrj-v574 **Recommendation** Fix available in 4.17.11 **References** https://hackerone.com/reports/380873 https://security.netapp.com/advisory/ntap-20190919-0004/ https://hackerone.com/reports/380873 https://security.netapp.com/advisory/ntap-20190919-0004/ **CVE:** CVE-2018-16487 - **CVSS**: null
pkg:npm/markdown-it-katex@%5E2.0.3 version >=0.0.0 (unknown)	HV-GHSA-5ff8-jcf9-fw62	**Overview** Cross-Site Scripting in markdown-it-katex **Grype Data Source**: https://github.com/advisories/GHSA-5ff8-jcf9-fw62

		Recommendation Fix available in None Provided **References** None Provided **CVE:** None Provided - **CVSS**: null
pkg:npm/markdown-it-katex@2.0.3 version >=0.0.0 (unknown)	HV-GHSA-5ff8-jcf9-fw62	**Overview** Cross-Site Scripting in markdown-it-katex **Grype Data Source**: https://github.com/advisories/GHSA-5ff8-jcf9-fw62 **Recommendation** Fix available in None Provided **References** None Provided **CVE:** None Provided - **CVSS**: null
pkg:npm/ws@%5E8.6.0 version >=0.2.6, <1.1.5 (unknown)	HV-GHSA-5v72-xg48-5rpm	**Overview** Denial of Service in ws **Grype Data Source**: https://github.com/advisories/GHSA-5v72-xg48-5rpm **Recommendation** Fix available in 1.1.5 **References** None Provided **CVE:** None Provided - **CVSS**: 7.5
pkg:npm/ws@%5E8.6.0 version <1.1.1 (unknown)	HV-GHSA-6663-c963-2gqg	**Overview** DoS due to excessively large websocket message in ws **Grype Data Source**: https://github.com/advisories/GHSA-6663-c963-2gqg **Recommendation** Fix available in 1.1.1 **References** https://github.com/nodejs/node/issues/7388 https://nodesecurity.io/advisories/120 https://github.com/nodejs/node/issues/7388 https://nodesecurity.io/advisories/120 **CVE:** CVE-2016-10542 - **CVSS**: null
pkg:npm/canvas@%5E2.8.0 version <1.6.11 (unknown)	HV-GHSA-73rg-x683-m3qw	**Overview** Buffer overflow in canvas **Grype Data Source**: https://github.com/advisories/GHSA-73rg-x683-m3qw **Recommendation** Fix available in 1.6.11 **References** https://hackerone.com/reports/315037 https://hackerone.com/reports/315037 **CVE:** CVE-2020-8215 - **CVSS**: 8.8
pkg:npm/trim-newlines@1.0.0 version <3.0.1 (unknown)	HV-GHSA-7p7h-4mm5-852v	**Overview** Uncontrolled Resource Consumption in trim-newlines **Grype Data Source**: https://github.com/advisories/GHSA-7p7h-4mm5-852v **Recommendation** Fix available in 3.0.1 **References** https://github.com/sindresorhus/trim-newlines/releases/tag/v4.0.1 https://lists.debian.org/debian-lts-announce/2022/12/msg00033.html https://security.netapp.com/advisory/ntap-20210702-0007/ https://www.npmjs.com/package/trim-newlines https://github.com/sindresorhus/trim-newlines/releases/tag/v4.0.1 https://lists.debian.org/debian-lts-announce/2022/12/msg00033.html https://security.netapp.com/advisory/ntap-20210702-0007/ https://www.npmjs.com/package/trim-newlines **CVE:** CVE-2021-33623 - **CVSS**: 7.5
pkg:npm/trim-newlines@2.0.0 version <3.0.1 (unknown)	HV-GHSA-7p7h-4mm5-852v	**Overview** Uncontrolled Resource Consumption in trim-newlines **Grype Data Source**: https://github.com/advisories/GHSA-7p7h-4mm5-852v **Recommendation** Fix available in 3.0.1 **References** https://github.com/sindresorhus/trim-newlines/releases/tag/v4.0.1 https://lists.debian.org/debian-lts-announce/2022/12/msg00033.html https://security.netapp.com/advisory/ntap-20210702-0007/ https://www.npmjs.com/package/trim-newlines https://github.com/sindresorhus/trim-newlines/releases/tag/v4.0.1 https://lists.debian.org/debian-lts-announce/2022/12/msg00033.html https://security.netapp.com/advisory/ntap-20210702-0007/ https://www.npmjs.com/package/trim-newlines **CVE:** CVE-2021-33623 - **CVSS**: 7.5
pkg:npm/ansi-regex@3.0.0 version >=3.0.0, <3.0.1 (unknown)	HV-GHSA-93q8-gq69-wqmw	**Overview** Inefficient Regular Expression Complexity in chalk/ansi-regex **Grype Data Source**: https://github.com/advisories/GHSA-93q8-gq69-wqmw **Recommendation** Fix available in 3.0.1 **References** https://github.com/chalk/ansi-regex/commit/8d1d7cdb586269882c4bdc1b7325d0c58c8f76f9 https://huntr.dev/bounties/5b3cf33b-ede0-4398-9974-800876dfd994 https://security.netapp.com/advisory/ntap-20221014-0002/

		https://www.oracle.com/security-alerts/cpuapr2022.html https://github.com/chalk/ansi-regex/commit/8d1d7cdb586269882c4bdc1b7325d0c58c8f76f9 https://huntr.dev/bounties/5b3cf33b-ede0-4398-9974-800876dfd994 https://security.netapp.com/advisory/ntap-20221014-0002/ https://www.oracle.com/security-alerts/cpuapr2022.html **CVE:** CVE-2021-3807 - **CVSS**: 7.5
pkg:npm/ansi-regex@4.1.0 version >=4.0.0, <4.1.1 (unknown)	HV-GHSA-93q8-gq69-wqmw	**Overview** Inefficient Regular Expression Complexity in chalk/ansi-regex **Grype Data Source**: https://github.com/advisories/GHSA-93q8-gq69-wqmw **Recommendation** Fix available in 4.1.1 **References** https://github.com/chalk/ansi-regex/commit/8d1d7cdb586269882c4bdc1b7325d0c58c8f76f9 https://huntr.dev/bounties/5b3cf33b-ede0-4398-9974-800876dfd994 https://security.netapp.com/advisory/ntap-20221014-0002/ https://www.oracle.com/security-alerts/cpuapr2022.html https://github.com/chalk/ansi-regex/commit/8d1d7cdb586269882c4bdc1b7325d0c58c8f76f9 https://huntr.dev/bounties/5b3cf33b-ede0-4398-9974-800876dfd994 https://security.netapp.com/advisory/ntap-20221014-0002/ https://www.oracle.com/security-alerts/cpuapr2022.html **CVE:** CVE-2021-3807 - **CVSS**: 7.5
pkg:npm/rollup@%5E4.24.0 version <2.79.2 (unknown)	HV-GHSA-gcx4-mw62-g8wm	**Overview** DOM Clobbering Gadget found in rollup bundled scripts that leads to XSS **Grype Data Source**: https://github.com/advisories/GHSA-gcx4-mw62-g8wm **Recommendation** Fix available in 2.79.2 **References** https://github.com/rollup/rollup/blob/b86ffd776cfa906573d36c3f019316d02445d9ef/src/ast/nodes/MetaProperty.ts#L157-L162 https://github.com/rollup/rollup/blob/b86ffd776cfa906573d36c3f019316d02445d9ef/src/ast/nodes/MetaProperty.ts#L180-L185 https://github.com/rollup/rollup/commit/2ef77c00ec2635d42697cff2c0567ccc8db34fb4 https://github.com/rollup/rollup/commit/e2552c9e955e0a61f70f508200ee9f752f85a541 https://github.com/rollup/rollup/security/advisories/GHSA-gcx4-mw62-g8wm **CVE:** CVE-2024-47068 - **CVSS**: 6.4
pkg:npm/prismjs@%5E1.29.0 version <1.24.0 (unknown)	HV-GHSA-gj77-59wh-66hg	**Overview** Regular Expression Denial of Service (ReDoS) in Prism **Grype Data Source**: https://github.com/advisories/GHSA-gj77-59wh-66hg **Recommendation** Fix available in 1.24.0 **References** https://github.com/PrismJS/prism/pull/2688 https://github.com/PrismJS/prism/pull/2774 https://github.com/PrismJS/prism/security/advisories/GHSA-gj77-59wh-66hg https://www.oracle.com/security-alerts/cpujan2022.html https://github.com/PrismJS/prism/pull/2688 https://github.com/PrismJS/prism/pull/2774 https://github.com/PrismJS/prism/security/advisories/GHSA-gj77-59wh-66hg https://www.oracle.com/security-alerts/cpujan2022.html **CVE:** CVE-2021-32723 - **CVSS**: 7.4
pkg:npm/braces@2.3.2 version <3.0.3 (unknown)	HV-GHSA-grv7-fg5c-xmjg	**Overview** Uncontrolled resource consumption in braces **Grype Data Source**: https://github.com/advisories/GHSA-grv7-fg5c-xmjg **Recommendation** Fix available in 3.0.3 **References** https://devhub.checkmarx.com/cve-details/CVE-2024-4068/ https://github.com/micromatch/braces/commit/415d660c3002d1ab7e63dbf490c9851da80596ff https://github.com/micromatch/braces/issues/35 https://github.com/micromatch/braces/pull/37 https://github.com/micromatch/braces/pull/40 https://devhub.checkmarx.com/cve-details/CVE-2024-4068/ https://github.com/micromatch/braces/commit/415d660c3002d1ab7e63dbf490c9851da80596ff https://github.com/micromatch/braces/issues/35 https://github.com/micromatch/braces/pull/37 https://github.com/micromatch/braces/pull/40 **CVE:** CVE-2024-4068 - **CVSS**: 7.5
pkg:npm/braces@3.0.2 version <3.0.3 (unknown)	HV-GHSA-grv7-fg5c-xmjg	**Overview** Uncontrolled resource consumption in braces **Grype Data Source**: https://github.com/advisories/GHSA-grv7-fg5c-xmjg **Recommendation** Fix available in 3.0.3 **References** https://devhub.checkmarx.com/cve-details/CVE-2024-4068/ https://github.com/micromatch/braces/commit/415d660c3002d1ab7e63dbf490c9851da80596ff https://github.com/micromatch/braces/issues/35 https://github.com/micromatch/braces/pull/37 https://github.com/micromatch/braces/pull/40 https://devhub.checkmarx.com/cve-details/CVE-2024-4068/ https://github.com/micromatch/braces/commit/415d660c3002d1ab7e63dbf490c9851da80596ff https://github.com/micromatch/braces/issues/35 https://github.com/micromatch/braces/pull/37 https://github.com/micromatch/braces/pull/40 **CVE:** CVE-2024-4068 - **CVSS**: 7.5
pkg:npm/prismjs@%5E1.29.0 version <1.23.0 (unknown)	HV-GHSA-h4hr-7fg3-h35w	**Overview** Denial of service in prismjs **Grype Data Source**: https://github.com/advisories/GHSA-h4hr-7fg3-h35w

		Recommendation Fix available in 1.23.0 **References** https://github.com/PrismJS/prism/commit/c2f6a64426f44497a675cb32dccb079b3eff1609 https://github.com/PrismJS/prism/issues/2583 https://github.com/PrismJS/prism/pull/2584 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1076583 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1076582 https://snyk.io/vuln/SNYK-JS-PRISMJS-1076581 https://github.com/PrismJS/prism/commit/c2f6a64426f44497a675cb32dccb079b3eff1609 https://github.com/PrismJS/prism/issues/2583 https://github.com/PrismJS/prism/pull/2584 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-1076583 https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1076582 https://snyk.io/vuln/SNYK-JS-PRISMJS-1076581 **CVE:** CVE-2021-23341 - **CVSS**: null
pkg:npm/markdown-it@%5E13.0.1 version <3.0.0 (unknown)	HV-GHSA-j5p7-jf4q-742q	**Overview** markdown-it vulnerable to Inefficient Regular Expression Complexity **Grype Data Source**: https://github.com/advisories/GHSA-j5p7-jf4q-742q **Recommendation** Fix available in 3.0.0 **References** https://github.com/markdown-it/markdown-it/commit/89c8620157d6e38f9872811620d25138fc9d1b0d https://github.com/markdown-it/markdown-it/releases/tag/3.0.0 https://vuldb.com/?ctiid.216852 https://vuldb.com/?id.216852 https://github.com/markdown-it/markdown-it/commit/89c8620157d6e38f9872811620d25138fc9d1b0d https://github.com/markdown-it/markdown-it/releases/tag/3.0.0 https://vuldb.com/?ctiid.216852 https://vuldb.com/?id.216852 **CVE:** CVE-2015-10005 - **CVSS**: 7.5
pkg:npm/markdown-it@%5E14.1.0 version <3.0.0 (unknown)	HV-GHSA-j5p7-jf4q-742q	**Overview** markdown-it vulnerable to Inefficient Regular Expression Complexity **Grype Data Source**: https://github.com/advisories/GHSA-j5p7-jf4q-742q **Recommendation** Fix available in 3.0.0 **References** https://github.com/markdown-it/markdown-it/commit/89c8620157d6e38f9872811620d25138fc9d1b0d https://github.com/markdown-it/markdown-it/releases/tag/3.0.0 https://vuldb.com/?ctiid.216852 https://vuldb.com/?id.216852 https://github.com/markdown-it/markdown-it/commit/89c8620157d6e38f9872811620d25138fc9d1b0d https://github.com/markdown-it/markdown-it/releases/tag/3.0.0 https://vuldb.com/?ctiid.216852 https://vuldb.com/?id.216852 **CVE:** CVE-2015-10005 - **CVSS**: 7.5
pkg:npm/vite@%5E4 version <2.9.13 (unknown)	HV-GHSA-mv48-hcvh-8jj8	**Overview** Vite before v2.9.13 vulnerable to directory traversal via crafted URL to victim's service **Grype Data Source**: https://github.com/advisories/GHSA-mv48-hcvh-8jj8 **Recommendation** Fix available in 2.9.13 **References** https://github.com/vitejs/vite/issues/8498 https://github.com/vitejs/vite/releases/tag/v2.9.13 https://github.com/vitejs/vite/releases/tag/v3.0.0-beta.4 https://github.com/vitejs/vite/issues/8498 https://github.com/vitejs/vite/releases/tag/v2.9.13 https://github.com/vitejs/vite/releases/tag/v3.0.0-beta.4 **CVE:** CVE-2022-35204 - **CVSS**: 8.6
pkg:npm/vite@%5E4.0.4 version <2.9.13 (unknown)	HV-GHSA-mv48-hcvh-8jj8	**Overview** Vite before v2.9.13 vulnerable to directory traversal via crafted URL to victim's service **Grype Data Source**: https://github.com/advisories/GHSA-mv48-hcvh-8jj8 **Recommendation** Fix available in 2.9.13 **References** https://github.com/vitejs/vite/issues/8498 https://github.com/vitejs/vite/releases/tag/v2.9.13 https://github.com/vitejs/vite/releases/tag/v3.0.0-beta.4 https://github.com/vitejs/vite/issues/8498 https://github.com/vitejs/vite/releases/tag/v2.9.13 https://github.com/vitejs/vite/releases/tag/v3.0.0-beta.4 **CVE:** CVE-2022-35204 - **CVSS**: 8.6
pkg:npm/vite@%5E5.2.1 version <2.9.13 (unknown)	HV-GHSA-mv48-hcvh-8jj8	**Overview** Vite before v2.9.13 vulnerable to directory traversal via crafted URL to victim's service **Grype Data Source**: https://github.com/advisories/GHSA-mv48-hcvh-8jj8 **Recommendation** Fix available in 2.9.13 **References** https://github.com/vitejs/vite/issues/8498 https://github.com/vitejs/vite/releases/tag/v2.9.13 https://github.com/vitejs/vite/releases/tag/v3.0.0-beta.4 https://github.com/vitejs/vite/issues/8498 https://github.com/vitejs/vite/releases/tag/v2.9.13 https://github.com/vitejs/vite/releases/tag/v3.0.0-beta.4 **CVE:** CVE-2022-35204 - **CVSS**: 8.6
pkg:npm/lodash.set@4.3.2 version >=3.7.0, <=4.3.2 (unknown)	HV-GHSA-p6mc-m468-83gw	**Overview** Prototype Pollution in lodash **Grype Data Source**: https://github.com/advisories/GHSA-p6mc-m468-83gw

		Recommendation Fix available in None Provided **References** https://github.com/lodash/lodash/issues/4874 https://hackerone.com/reports/712065 https://security.netapp.com/advisory/ntap-20200724-0006/ https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpuApr2021.html https://www.oracle.com/security-alerts/cpuapr2022.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpuoct2021.html https://github.com/lodash/lodash/issues/4874 https://hackerone.com/reports/712065 https://security.netapp.com/advisory/ntap-20200724-0006/ https://www.oracle.com//security-alerts/cpujul2021.html https://www.oracle.com/security-alerts/cpuApr2021.html https://www.oracle.com/security-alerts/cpuapr2022.html https://www.oracle.com/security-alerts/cpujan2022.html https://www.oracle.com/security-alerts/cpuoct2021.html **CVE:** CVE-2020-8203 - **CVSS**: 7.4
pkg:npm/node-fetch@%5E3.3.1 version <2.6.7 (unknown)	HV-GHSA-r683-j2x4-v87g	**Overview** node-fetch forwards secure headers to untrusted sites **Grype Data Source**: https://github.com/advisories/GHSA-r683-j2x4-v87g **Recommendation** Fix available in 2.6.7 **References** https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/node-fetch/node-fetch/commit/36e47e8a6406185921e4985dcbeff140d73eaa10 https://huntr.dev/bounties/d26ab655-38d6-48b3-be15-f9ad6b6ae6f7 https://lists.debian.org/debian-lts-announce/2022/12/msg00007.html https://cert-portal.siemens.com/productcert/pdf/ssa-637483.pdf https://github.com/node-fetch/node-fetch/commit/36e47e8a6406185921e4985dcbeff140d73eaa10 https://huntr.dev/bounties/d26ab655-38d6-48b3-be15-f9ad6b6ae6f7 https://lists.debian.org/debian-lts-announce/2022/12/msg00007.html **CVE:** CVE-2022-0235 - **CVSS**: 8.8
pkg:npm/http-cache-semantics@3.8.1 version <4.1.1 (unknown)	HV-GHSA-rc47-6667-2j5j	**Overview** http-cache-semantics vulnerable to Regular Expression Denial of Service **Grype Data Source**: https://github.com/advisories/GHSA-rc47-6667-2j5j **Recommendation** Fix available in 4.1.1 **References** https://github.com/kornelski/http-cache-semantics/blob/master/index.js%23L83 https://security.netapp.com/advisory/ntap-20230622-0008/ https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3253332 https://security.snyk.io/vuln/SNYK-JS-HTTPCACHESEMANTICS-3248783 https://github.com/kornelski/http-cache-semantics/blob/master/index.js%23L83 https://security.netapp.com/advisory/ntap-20230622-0008/ https://security.snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-3253332 https://security.snyk.io/vuln/SNYK-JS-HTTPCACHESEMANTICS-3248783 **CVE:** CVE-2022-25881 - **CVSS**: 7.5
pkg:npm/path-to-regexp@0.1.10 version <0.1.12 (unknown)	HV-GHSA-rhx6-c78j-4q9w	**Overview** path-to-regexp contains a ReDoS **Grype Data Source**: https://github.com/advisories/GHSA-rhx6-c78j-4q9w **Recommendation** Fix available in 0.1.12 **References** https://github.com/pillarjs/path-to-regexp/commit/f01c26a013b1889f0c217c643964513acf17f6a4 https://github.com/pillarjs/path-to-regexp/security/advisories/GHSA-rhx6-c78j-4q9w https://security.netapp.com/advisory/ntap-20250124-0002/ **CVE:** CVE-2024-52798 - **CVSS**: 7.5
pkg:npm/decode-uri-component@0.2.0 version <0.2.1 (unknown)	HV-GHSA-w573-4hg7-7wgq	**Overview** decode-uri-component vulnerable to Denial of Service (DoS) **Grype Data Source**: https://github.com/advisories/GHSA-w573-4hg7-7wgq **Recommendation** Fix available in 0.2.1 **References** https://github.com/SamVerschueren/decode-uri-component/issues/5 https://github.com/sindresorhus/query-string/issues/345 https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ERN6YE3DS7NBW7UH44SCJBMNC2NWQ7SM/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KAC5KQ2SEWAMQ6UZAUBZ5KXKEOESH375/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/QABOUA2I542UTANVZIVFKWMRYVHLV32D/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UW4SCMT3SEUFVIL7YIADQ5K36GJEO6I5/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VNV2GNZXOTEDAJRFH3ZYWRUBGIVL7BSU/ https://github.com/SamVerschueren/decode-uri-component/issues/5 https://github.com/sindresorhus/query-string/issues/345 https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/ERN6YE3DS7NBW7UH44SCJBMNC2NWQ7SM/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/KAC5KQ2SEWAMQ6UZAUBZ5KXKEOESH375/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/QABOUA2I542UTANVZIVFKWMRYVHLV32D/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/UW4SCMT3SEUFVIL7YIADQ5K36GJEO6I5/ https://lists.fedoraproject.org/archives/list/package-announce%40lists.fedoraproject.org/message/VNV2GNZXOTEDAJRFH3ZYWRUBGIVL7BSU/ **CVE:** CVE-2022-38900 - **CVSS**: 7.5

Critical and High maliciousCodeRisk

Package	Impact	Description

Critical and High engineeringRisk

Package	Impact	Description

Critical and High authorsRisk

Package	Impact	Description

Critical, High, Medium, and Low licenseRisk

Package	Impact	Description

> Created by pub-scir pubRel 250516evie (branch: publicRelease) on Wed Aug 13 12:50:57 UTC 2025

No labels