



OpenHack

Supply Chain Audit Report

Devil's Advocate

Organization: meridian-cloud

Generated: October 19, 2026 (UTC)

Generated by: ananay@openhack.com

Scan date: July 18, 2026 (UTC)

CONFIDENTIAL

Executive Risk Summary

Overall Risk: HIGH

This report summarizes a supply chain security analysis of the Devil's Advocate project. The scan analyzed 444 packages across 1 lockfile and identified 46 known vulnerabilities. 29 vulnerabilities affect direct dependencies.

Severity Breakdown

Critical 1	High 18	Medium 24	Low 3
---------------	------------	--------------	----------

Total Vulnerabilities: 46

Scan Coverage

Lockfiles found: 1
Lockfiles scanned: 1
Total packages: 444
Direct dependencies: 26
Transitive dependencies: 418
Ecosystems: npm

Lockfiles Scanned

- package-lock.json

Remediation Trail

New 46	Persisting 0	Resolved 0
-----------	-----------------	---------------

Dependency Classification

Direct dependency vulnerabilities: 29
Transitive dependency vulnerabilities: 17

Direct Dependency Vulnerabilities (Priority)

- [CRITICAL] GHSA-f82v-jwr5-mffw - next@14.0.4
- [HIGH] GHSA-36qx-fr4f-26g5 - next@14.0.4
- [HIGH] GHSA-5j59-xgg2-r9c4 - next@14.0.4
- [HIGH] GHSA-7gfc-8cq8-jh5f - next@14.0.4
- [HIGH] GHSA-8h8q-6873-q5fj - next@14.0.4
- [HIGH] GHSA-c4j6-fc7j-m34r - next@14.0.4
- [HIGH] GHSA-fr5h-rqp8-mj6g - next@14.0.4

[HIGH] GHSA-gp8f-8m3g-qvj9 - next@14.0.4
[HIGH] GHSA-h25m-26qc-wcjf - next@14.0.4
[HIGH] GHSA-mwv6-3258-q52c - next@14.0.4
[HIGH] GHSA-q4gf-8mx6-v5v3 - next@14.0.4
[HIGH] GHSA-w5hq-g745-h8pq - uuid@9.0.1
[MEDIUM] GHSA-pxg6-pf52-xh8x - cookie@0.6.0
[MEDIUM] GHSA-3h52-269p-cp9r - next@14.0.4
[MEDIUM] GHSA-3x4c-7xq6-9pq8 - next@14.0.4
[MEDIUM] GHSA-4342-x723-ch2f - next@14.0.4
[MEDIUM] GHSA-7m27-7ghc-44w9 - next@14.0.4
[MEDIUM] GHSA-9g9p-9gw9-jx7f - next@14.0.4
[MEDIUM] GHSA-g77x-44xx-532m - next@14.0.4
[MEDIUM] GHSA-ffhc-5mcf-pf4q - next@14.0.4
... and 9 more

License Compliance

Packages with detected licenses: 198 of 444

License Distribution

MIT: 166
Apache-2.0: 16
ISC: 7
BSD-2-Clause: 4
BSD-3-Clause: 2
Python-2.0: 1
MPL-2.0: 1
CC-BY-4.0: 1

Dependency Health

Deprecated Packages (4)

- @humanwhocodes/object-schema@2.0.3 (npm)
Use @eslint/object-schema instead
- @ungap/structured-clone@1.3.0 (npm)
Potential CWE-502 - Update to 1.3.1 or higher
- @humanwhocodes/config-array@0.13.0 (npm)
Use @eslint/config-array instead
- eslint@8.57.1 (npm)
This version is no longer supported. Please see <https://eslint.org/version-support> for other options.

Exploitability Context

EPSS Exploitability Scores

EPSS (Exploit Prediction Scoring System) estimates the probability of exploitation within 30 days.

GHSA-f82v-jwr5-mffw: EPSS 99.30% (100th percentile) - next
GHSA-gp8f-8m3g-qvj9: EPSS 58.77% (99th percentile) - next
GHSA-c4j6-fc7j-m34r: EPSS 38.87% (98th percentile) - next
GHSA-fr5h-rqp8-mj6g: EPSS 5.45% (92th percentile) - next
GHSA-7gfc-8cq8-jh5f: EPSS 3.96% (89th percentile) - next
GHSA-4342-x723-ch2f: EPSS 2.33% (82th percentile) - next
GHSA-rf6f-7fwh-wjgh: EPSS 0.81% (53th percentile) - flatted
GHSA-25h7-pfq9-p65f: EPSS 0.81% (53th percentile) - flatted
GHSA-7m27-7ghc-44w9: EPSS 0.81% (53th percentile) - next
GHSA-pxg6-pf52-xh8x: EPSS 0.74% (51th percentile) - cookie
GHSA-g77x-44xx-532m: EPSS 0.74% (50th percentile) - next
GHSA-h64f-5h5j-jqjh: EPSS 0.72% (50th percentile) - next
GHSA-3x4c-7xq6-9pq8: EPSS 0.68% (48th percentile) - next
GHSA-qpvj-v59x-3qc4: EPSS 0.67% (48th percentile) - next
GHSA-36qx-fr4f-26g5: EPSS 0.61% (45th percentile) - next
GHSA-3ppc-4f35-3m26: EPSS 0.52% (41th percentile) - minimatch
GHSA-3ppc-4f35-3m26: EPSS 0.52% (41th percentile) - minimatch
GHSA-7r86-cg39-jmmj: EPSS 0.52% (41th percentile) - minimatch
GHSA-7r86-cg39-jmmj: EPSS 0.52% (41th percentile) - minimatch
GHSA-xv57-4mr9-wg8v: EPSS 0.51% (40th percentile) - next
... and 21 more with EPSS data

Prioritized Remediation Plan

Remediation actions grouped by package, sorted by impact. Each upgrade resolves all listed advisories.

1. next@14.0.4 → 15.5.16 BREAKING (direct)

Resolves 26 findings: CVE-2025-29927, CVE-2026-44573, GHSA-5j59-xgg2-r9c4, CVE-2024-51479, GHSA-8h8q-6873-q5fj, CVE-2026-44578, CVE-2024-34351, CVE-2024-46982, GHSA-h25m-26qc-wcjf, GHSA-mwv6-3258-q52c, GHSA-q4gf-8mx6-v5v3, CVE-2025-48068, CVE-2026-27980, CVE-2025-57822, CVE-2024-56332, CVE-2025-59471, CVE-2024-47831, CVE-2026-44581, CVE-2025-57752, CVE-2026-29057, CVE-2026-44580, CVE-2026-44577, CVE-2025-55173, CVE-2026-44572, CVE-2025-32421, CVE-2026-44582

2. minimatch@3.1.2 → 3.1.4 (transitive)

Resolves 3 findings: CVE-2026-27904, CVE-2026-27903, CVE-2026-26996

3. minimatch@9.0.3 → 9.0.7 (transitive)

Resolves 3 findings: CVE-2026-27904, CVE-2026-27903, CVE-2026-26996

4. flatted@3.3.3 → 3.4.2 (transitive)

Resolves 2 findings: CVE-2026-32141, CVE-2026-33228

5. picomatch@2.3.1 → 2.3.2 (transitive)

Resolves 2 findings: CVE-2026-33671, CVE-2026-33672

6. picomatch@4.0.3 → 4.0.4 (transitive)

Resolves 2 findings: CVE-2026-33671, CVE-2026-33672

7. uuid@9.0.1 → 11.1.1 BREAKING (direct)

Resolves 1 finding: CVE-2026-41907

8. ajv@6.12.6 → 6.14.0 (transitive)

Resolves 1 finding: CVE-2025-69873

9. brace-expansion@1.1.12 → 1.1.13 (transitive)

Resolves 1 finding: CVE-2026-33750

10. brace-expansion@2.0.2 → 2.0.3 (transitive)

Resolves 1 finding: CVE-2026-33750

11. cookie@0.6.0 → 0.7.0 (direct)

Resolves 1 finding: CVE-2024-47764

12. js-yaml@4.1.1 → 4.2.0 (transitive)

Resolves 1 finding: CVE-2026-53550

13. postcss@8.4.31 → 8.5.10 (transitive)

Resolves 1 finding: CVE-2026-41305

14. postcss@8.5.6 → 8.5.10 (direct)

Resolves 1 finding: CVE-2026-41305

Vulnerability Findings

next @ 14.0.4

Ecosystem: npm | Vulnerabilities: 26 | Direct

[CRITICAL (CVSS 9.1)] CVE-2025-29927 / GHSA-f82v-jwr5-mffw [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Authorization Bypass in Next.js Middleware

Fix: 14.2.25 · EPSS: 99.30%

Aliases: CVE-2025-29927

[HIGH (CVSS 7.5)] CVE-2026-44573 / GHSA-36qx-fr4f-26g5 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Next.js has a Middleware / Proxy bypass in Pages Router applications using i18n

Fix: 15.5.16 · EPSS: 0.61%

Aliases: CVE-2026-44573

[HIGH (CVSS 7.5)] GHSA-5j59-xgg2-r9c4 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Next has a Denial of Service with Server Components - Incomplete Fix Follow-Up

Fix: 14.2.35

[HIGH (CVSS 7.5)] CVE-2024-51479 / GHSA-7gfc-8cq8-jh5f [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Next.js authorization bypass vulnerability

Fix: 14.2.15 · EPSS: 3.96%

Aliases: CVE-2024-51479

[HIGH (CVSS 7.5)] GHSA-8h8q-6873-q5fj [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Next.js Vulnerable to Denial of Service with Server Components

Fix: 15.5.16

[HIGH (CVSS 8.6)] CVE-2026-44578 / GHSA-c4j6-fc7j-m34r [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Next.js vulnerable to server-side request forgery in applications using WebSocket upgrades

Fix: 15.5.16 · EPSS: 38.87%

Aliases: CVE-2026-44578

[HIGH (CVSS 7.5)] CVE-2024-34351 / GHSA-fr5h-rqp8-mj6g [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Next.js Server-Side Request Forgery in Server Actions

Fix: 14.1.1 · EPSS: 5.45%

Aliases: CVE-2024-34351

[HIGH (CVSS 7.5)] CVE-2024-46982 / GHSA-gp8f-8m3g-qvj9 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Next.js Cache Poisoning

Fix: 14.2.10 · EPSS: 58.77%

Aliases: CVE-2024-46982

[HIGH (CVSS 7.5)] GHSA-h25m-26qc-wcjf [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Next.js HTTP request deserialization can lead to DoS when using insecure React Server Components

Fix: 15.0.8

[HIGH (CVSS 7.5)] GHSA-mwv6-3258-q52c [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Next Vulnerable to Denial of Service with Server Components

Fix: 14.2.34

[HIGH (CVSS 7.5)] GHSA-q4gf-8mx6-v5v3 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Next.js has a Denial of Service with Server Components

Fix: 15.5.15

[UNRATED] CVE-2025-48068 / GHSA-3h52-269p-cp9r [NEW]

Information exposure in Next.js dev server due to lack of origin verification

Fix: 14.2.30 · EPSS: 0.17%

Aliases: CVE-2025-48068

[UNRATED] CVE-2026-27980 / GHSA-3x4c-7xq6-9pq8 [NEW]

Next.js: Unbounded next/image disk cache growth can exhaust storage

Fix: 15.5.14 · EPSS: 0.68%

Aliases: CVE-2026-27980

[MEDIUM (CVSS 6.5)] CVE-2025-57822 / GHSA-4342-x723-ch2f [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N

Next.js Improper Middleware Redirect Handling Leads to SSRF

Fix: 14.2.32 · EPSS: 2.33%

Aliases: CVE-2025-57822

[MEDIUM (CVSS 5.3)] CVE-2024-56332 / GHSA-7m27-7ghc-44w9 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Next.js Allows a Denial of Service (DoS) with Server Actions

Fix: 14.2.21 · EPSS: 0.81%

Aliases: CVE-2024-56332

[MEDIUM (CVSS 5.9)] CVE-2025-59471 / GHSA-9g9p-9gw9-jx7f [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Next.js self-hosted applications vulnerable to DoS via Image Optimizer remotePatterns configuration

Fix: 15.5.10 · EPSS: 0.44%

Aliases: CVE-2025-59471

[MEDIUM (CVSS 5.9)] CVE-2024-47831 / GHSA-g77x-44xx-532m [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Denial of Service condition in Next.js image optimization

Fix: 14.2.7 · EPSS: 0.74%

Aliases: CVE-2024-47831

[MEDIUM (CVSS 4.7)] CVE-2026-44581 / GHSA-ffhc-5mcf-pf4q [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/L/I:L/A:N

Next.js vulnerable to cross-site scripting in App Router applications using CSP nonces

Fix: 15.5.16 · EPSS: 0.22%

Aliases: CVE-2026-44581

[MEDIUM (CVSS 6.2)] CVE-2025-57752 / GHSA-g5qg-72qw-gw5v [NEW]

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Next.js Affected by Cache Key Confusion for Image Optimization API Routes

Fix: 14.2.31 · EPSS: 0.33%

Aliases: CVE-2025-57752

[UNRATED] CVE-2026-29057 / GHSA-ggv3-7p47-pfv8 [NEW]

Next.js: HTTP request smuggling in rewrites

Fix: 15.5.13 · EPSS: 0.43%

Aliases: CVE-2026-29057

[MEDIUM (CVSS 6.1)] CVE-2026-44580 / GHSA-gx5p-jg67-6x7h [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/L/I:L/A:N

Next.js has cross-site scripting in beforeInteractive scripts with untrusted input

Fix: 15.5.16 · EPSS: 0.21%

Aliases: CVE-2026-44580

[MEDIUM (CVSS 5.9)] CVE-2026-44577 / GHSA-h64f-5h5j-jqjh [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Next.js has a Denial of Service in the Image Optimization API

Fix: 15.5.16 · EPSS: 0.72%

Aliases: CVE-2026-44577

[MEDIUM (CVSS 4.3)] CVE-2025-55173 / GHSA-xv57-4mr9-wg8v [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Next.js Content Injection Vulnerability for Image Optimization

Fix: 14.2.31 · EPSS: 0.51%

Aliases: CVE-2025-55173

[LOW (CVSS 3.7)] CVE-2026-44572 / GHSA-3g8h-86w9-wvmq [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L

Next.js's Middleware / Proxy redirects can be cache-poisoned

Fix: 15.5.16 · EPSS: 0.19%

Aliases: CVE-2026-44572

[LOW (CVSS 3.7)] CVE-2025-32421 / GHSA-qpvj-v59x-3qc4 [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Next.js Race Condition to Cache Poisoning

Fix: 14.2.24 · EPSS: 0.67%

Aliases: CVE-2025-32421

[LOW (CVSS 3.7)] CVE-2026-44582 / GHSA-vfv6-92ff-j949 [NEW]

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

Next.js vulnerable to cache poisoning via collisions in React Server Component cache-busting

Fix: 15.5.16 · EPSS: 0.20%

Aliases: CVE-2026-44582

flatted @ 3.3.3

Ecosystem: npm | Vulnerabilities: 2 | Transitive

[HIGH (CVSS 7.5)] CVE-2026-32141 / GHSA-25h7-pfq9-p65f [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

flatted vulnerable to unbounded recursion DoS in parse() revive phase

Fix: 3.4.0 · EPSS: 0.81%

Aliases: CVE-2026-32141

[UNRATED] CVE-2026-33228 / GHSA-rf6f-7fwh-wjgh [NEW]

Prototype Pollution via parse() in NodeJS flatted

Fix: 3.4.2 · EPSS: 0.81%

Aliases: CVE-2026-33228

minimatch @ 3.1.2

Ecosystem: npm | Vulnerabilities: 3 | Transitive

[HIGH (CVSS 7.5)] CVE-2026-27904 / GHSA-23c5-xmqv-rm74 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions

Fix: 3.1.4 · EPSS: 0.47%

Aliases: CVE-2026-27904

[HIGH (CVSS 7.5)] CVE-2026-27903 / GHSA-7r86-cg39-jmmj [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments

Fix: 3.1.3 · EPSS: 0.52%

Aliases: CVE-2026-27903

[UNRATED] CVE-2026-26996 / GHSA-3ppc-4f35-3m26 [NEW]

minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern

Fix: 3.1.3 · EPSS: 0.52%

Aliases: CVE-2026-26996

minimatch @ 9.0.3

Ecosystem: npm | Vulnerabilities: 3 | Transitive | License: ISC

[HIGH (CVSS 7.5)] CVE-2026-27904 / GHSA-23c5-xmqv-rm74 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

minimatch ReDoS: nested *() extglobs generate catastrophically backtracking regular expressions

Fix: 9.0.7 · EPSS: 0.47%

Aliases: CVE-2026-27904

[HIGH (CVSS 7.5)] CVE-2026-27903 / GHSA-7r86-cg39-jmmj [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

minimatch has ReDoS: matchOne() combinatorial backtracking via multiple non-adjacent GLOBSTAR segments

Fix: 9.0.7 · EPSS: 0.52%

Aliases: CVE-2026-27903

[UNRATED] CVE-2026-26996 / GHSA-3ppc-4f35-3m26 [NEW]

minimatch has a ReDoS via repeated wildcards with non-matching literal in pattern

Fix: 9.0.6 · EPSS: 0.52%

Aliases: CVE-2026-26996

picomatch @ 2.3.1

Ecosystem: npm | Vulnerabilities: 2 | Transitive

[HIGH (CVSS 7.5)] CVE-2026-33671 / GHSA-c2c7-rcm5-vvqj [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Picomatch has a ReDoS vulnerability via extglob quantifiers

Fix: 2.3.2 · EPSS: 0.41%

Aliases: CVE-2026-33671

[MEDIUM (CVSS 5.3)] CVE-2026-33672 / GHSA-3v7f-55p6-f55p [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Picomatch: Method Injection in POSIX Character Classes causes incorrect Glob Matching

Fix: 2.3.2 · EPSS: 0.41%

Aliases: CVE-2026-33672

picomatch @ 4.0.3

Ecosystem: npm | Vulnerabilities: 2 | Transitive

[HIGH (CVSS 7.5)] CVE-2026-33671 / GHSA-c2c7-rcm5-vvqj [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Picomatch has a ReDoS vulnerability via extglob quantifiers

Fix: 4.0.4 · EPSS: 0.41%

Aliases: CVE-2026-33671

[MEDIUM (CVSS 5.3)] CVE-2026-33672 / GHSA-3v7f-55p6-f55p [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Picomatch: Method Injection in POSIX Character Classes causes incorrect Glob Matching

Fix: 4.0.4 · EPSS: 0.41%

Aliases: CVE-2026-33672

uuid @ 9.0.1

Ecosystem: npm | Vulnerabilities: 1 | Direct

[HIGH (CVSS 7.5)] CVE-2026-41907 / GHSA-w5hq-g745-h8pq [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

uuid: Missing buffer bounds check in v3/v5/v6 when buf is provided

Fix: 11.1.1 · EPSS: 0.34%

Aliases: CVE-2026-41907, CVE-2026-41988

ajv @ 6.12.6

Ecosystem: npm | Vulnerabilities: 1 | Transitive | License: MIT

[UNRATED] CVE-2025-69873 / GHSA-2g4f-4pwh-qvx6 [NEW]

ajv has ReDoS when using `\$data` option

Fix: 6.14.0 · EPSS: 0.49%

Aliases: CVE-2025-69873

brace-expansion @ 1.1.12

Ecosystem: npm | Vulnerabilities: 1 | Transitive | License: MIT

[MEDIUM (CVSS 6.5)] CVE-2026-33750 / GHSA-f886-m6hf-6m8v [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

brace-expansion: Zero-step sequence causes process hang and memory exhaustion

Fix: 1.1.13 · EPSS: 0.43%

Aliases: CVE-2026-33750

brace-expansion @ 2.0.2

Ecosystem: npm | Vulnerabilities: 1 | Transitive | License: MIT

[MEDIUM (CVSS 6.5)] CVE-2026-33750 / GHSA-f886-m6hf-6m8v [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

brace-expansion: Zero-step sequence causes process hang and memory exhaustion

Fix: 2.0.3 · EPSS: 0.43%

Aliases: CVE-2026-33750

cookie @ 0.6.0

Ecosystem: npm | Vulnerabilities: 1 | Direct | License: MIT

[UNRATED] CVE-2024-47764 / GHSA-pxg6-pf52-xh8x [NEW]

cookie accepts cookie name, path, and domain with out of bounds characters

Fix: 0.7.0 · EPSS: 0.74%

Aliases: CVE-2024-47764

js-yaml @ 4.1.1

Ecosystem: npm | Vulnerabilities: 1 | Transitive

[MEDIUM (CVSS 5.3)] CVE-2026-53550 / GHSA-h67p-54hq-rp68 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

JS-YAML: Quadratic-complexity DoS in merge key handling via repeated aliases

Fix: 4.2.0 · EPSS: 0.26%

Aliases: CVE-2026-53550

postcss @ 8.4.31

Ecosystem: npm | Vulnerabilities: 1 | Transitive

[MEDIUM (CVSS 6.1)] CVE-2026-41305 / GHSA-qx2v-qp2m-jg93 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

PostCSS has XSS via Unescaped </style> in its CSS Stringify Output

Fix: 8.5.10 · EPSS: 0.21%

Aliases: CVE-2026-41305

postcss @ 8.5.6

Ecosystem: npm | Vulnerabilities: 1 | Direct

[MEDIUM (CVSS 6.1)] CVE-2026-41305 / GHSA-qx2v-qp2m-jg93 [NEW]

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

PostCSS has XSS via Unescaped </style> in its CSS Stringify Output

Fix: 8.5.10 · EPSS: 0.21%

Aliases: CVE-2026-41305

Methodology & Disclaimer

Scan Methodology

Dependencies were identified by parsing lockfiles from the repository. Each dependency was checked against the OSV (Open Source Vulnerabilities) database for known advisories. Severity levels are derived from CVSS v3.1 base scores when available: Critical (9.0-10.0), High (7.0-8.9), Medium (4.0-6.9), Low (0.1-3.9). Findings without a published CVSS score are labeled Unrated.

Risk Rating

The overall risk level is computed as: HIGH if any finding has Critical severity; MODERATE if there are more than 3 High-severity findings or any finding has an EPSS exploitation probability above 10%; LOW otherwise. This is an automated heuristic — manual review is recommended.

Data Sources

- Vulnerability advisories: OSV (Open Source Vulnerabilities) database
- Exploitability scores: FIRST.org Exploit Prediction Scoring System (EPSS)
- Package metadata: Ecosystem registries (npm, PyPI, crates.io, etc.)

Disclaimer

This report was generated automatically by OpenHack. Findings reflect the state of dependencies at the time of the scan and may not account for vulnerabilities disclosed afterward. This report is intended for internal audit and compliance purposes and does not constitute a guarantee of security.

Scan Metadata

Report ID: 2f37286a-256f-439c-b63d-37fde473096f
Commit: 3eb5c1448a503c6d7e3af5012719234d9fcde29b
Branch: main
Scan completed: 2026-07-18T01:38:09.111Z
Report generated: 2026-10-19T11:28:20.499Z
Engine: osv-scanner