Cross-site OpenCode server upgrade request can install arbitrary packages for npm-based installations

PRIMARY

Publisher	GitHub Security Advisories / anomalyco opencode
Published	2026-09-24
Retrieved	2026-09-29
Cite key	githubsecur2026crosssite
URL	https://github.com/anomalyco/opencode/security/advisories/GHSA-632h-h47v-g4x4

Cross-site OpenCode server upgrade request can install arbitrary packages for npm-based installations

GHSA-632h-h47v-g4x4 · GitHub Security Advisories · repository anomalyco/opencode · published 24 September 2026.

Severity: High, CVSS 7.5. Reporter credited: christophetd.

Package: `opencode-ai` (npm). Affected versions: from 1.14.30. Patched version: 1.18.22.

Description (as published)

"A webpage can submit a cross-site request to `/global/upgrade`" without proper origin validation. The endpoint accepts package specifiers that npm interprets as remote tarballs, allowing an attacker to specify a malicious package. The attack leverages browsers' handling of `text/plain` form submissions, which bypass cross-origin restrictions while still reaching the vulnerable endpoint.

Conditions required

- Victim runs `opencode serve`.
- OpenCode installed via npm, pnpm or Bun.
- The browser can reach the server.
- The victim visits an attacker-controlled webpage.

Weaknesses

CWE-346 (Origin Validation Error), CWE-352 (Cross-Site Request Forgery), CWE-436 (Interpretation Conflict).

Resolution

Version 1.18.22 implements strict content-type validation, semantic-version requirements for the upgrade target, and corrected request-body handling to prevent alternate package sources.

Note on adjacent identifiers

The same repository carries two earlier, distinct advisories published 12 January 2026: GHSA-vxw4-wv6m-9hhh, "Unauthenticated HTTP Server Allows Arbitrary Command Execution" (CVE-2026-22812), and GHSA-c83v-7274-4vgp, "Malicious website can execute commands on the local system through XSS in the OpenCode web UI" (CVE-2026-22813), the latter affecting releases before 1.1.10. These are not this advisory.