Discovering and exploiting a remote code execution vulnerability in OpenCode (GHSA-632h-h47v-g4x4)

PRIMARY

Publisher	Datadog Security Labs
Published	2026-09-24
Retrieved	2026-09-29
Cite key	datadogsecu2026discoveri
URL	https://securitylabs.datadoghq.com/articles/opencode-upgrade-remote-code-execution/

Discovering and exploiting a remote code execution vulnerability in OpenCode (GHSA-632h-h47v-g4x4)

Datadog Security Labs, Christophe Tafani-Dereeper, 24 September 2026.

Timeline (as published)

- 29 April 2026 — vulnerable code introduced via PR #24853.
- 30 April 2026 — first vulnerable release, v1.14.30.
- 11 August 2026 — Datadog Security Labs discovers the vulnerability and reports it through GitHub Security Advisories.
- 24 August 2026 — fix merged (PR #44686); v1.18.22 released with the patch.
- 24 September 2026 — public disclosure; official advisory published.

Affected and patched

Affected: OpenCode 1.14.30 through 1.18.21 — 82 vulnerable versions. Patched: v1.18.22 and later. Installation methods affected: npm, pnpm and Bun only.

Mechanism

1. Content-type confusion. The `/global/upgrade` endpoint parses the request body as JSON without

verifying the `Content-Type` header, so it accepts `text/plain` form submissions containing valid JSON.

2. npm specifier abuse. The vulnerable code executes `npm install -g opencode-ai@${target}`, and npm

interprets `target` as a package specifier, which may be a semantic version OR a URL pointing to a tarball.

3. Cross-origin exploitation. An attacker hosts a page with an HTML form using `enctype="text/plain"`,

crafting parameter names and values so the submitted body is valid JSON; browsers permit top-level cross-origin POST navigations.

4. Arbitrary code execution. The attacker-supplied tarball carries a malicious `preinstall` script in

package.json, which executes during installation.

Form injection example given in the article: the parameter NAME is a JSON fragment opening `target` and pointing it at an attacker-hosted `.tgz` over plain HTTP, and the parameter VALUE closes the object, so the submitted body parses as valid JSON. The literal scheme is omitted here because the archiver auto-links bare URLs inside code spans (see D85).

Exploitation requirements

- Victim runs OpenCode 1.14.30-1.18.21.
- OpenCode runs via `opencode serve` or `opencode web` without password authentication (or with cached credentials).
- OpenCode installed through npm, pnpm or Bun.
- Victim visits an attacker-controlled webpage from a browser that can reach the server.

Propagation

Weekly downloads of vulnerable versions, 17-23 September 2026: more than 647,000 — 38.9% of all OpenCode downloads in that period. The article states no unique-user count and makes no claim about exploitation in the wild.

Resolution

Version 1.18.22 adds strict content-type validation, requires the target to be a semantic version, and corrects request-body handling so alternate package sources cannot be supplied.