Source dossier

The update was the door — OpenCode's own upgrade endpoint installed the attacker's package, and the CRA limb that reaches it is not live until 2027

Edition 2026-09-29 · narrative: The duty that is live reports; the duty that would have closed this does not bind until 11 December 2027, so today the control is the engineer's. · compiled 2026-09-29

Claims index

Claim	Statement	Status	Sources
CLAIM-2026-09-29-01	GitHub advisory GHSA-632h-h47v-g4x4, published 24 September 2026, records that a webpage could submit a cross-site request to the OpenCode HTTP server's /global/upgrade endpoint and cause installation of an attacker-specified package; rated High, CVSS 7.5, with CWE-346, CWE-352 and CWE-436.	verified	githubsecur2026crosssite, datadogsecu2026discoveri
CLAIM-2026-09-29-02	Datadog Security Labs reports the affected range as OpenCode 1.14.30 through 1.18.21 - 82 releases - with the fix in v1.18.22; the vulnerable code was introduced on 29 April 2026 and first released on 30 April 2026 in v1.14.30.	verified	datadogsecu2026discoveri, githubsecur2026crosssite
CLAIM-2026-09-29-03	Datadog Security Labs discovered the flaw on 11 August 2026 and reported it through GitHub Security Advisories; the fix was merged and v1.18.22 released on 24 August 2026; public disclosure followed on 24 September 2026.	verified	datadogsecu2026discoveri
CLAIM-2026-09-29-04	In the week of 17-23 September 2026, Datadog measured more than 647,000 weekly downloads of vulnerable OpenCode versions, which it puts at 38.9% of all OpenCode downloads in that period.	verified	datadogsecu2026discoveri
CLAIM-2026-09-29-05	The mechanism is a content-type confusion: the /global/upgrade endpoint parsed the request body as JSON without validating Content-Type, so an HTML form with enctype text/plain - which browsers permit cross-origin - reached it, and the endpoint then ran npm install -g opencode-ai@${target} where npm interprets the target as a package specifier that may be a URL to a tarball, whose preinstall script executes.	verified	datadogsecu2026discoveri
CLAIM-2026-09-29-06	Exploitation requires that the victim runs OpenCode 1.14.30-1.18.21 via opencode serve or opencode web without password authentication, installed through npm, pnpm or Bun, and visits an attacker-controlled webpage from a browser that can reach the server.	verified	datadogsecu2026discoveri, githubsecur2026crosssite

Claim	Statement	Status	Sources
CLAIM-2026-09-29-07	The Cyber Resilience Act's Article 14 reporting obligations apply from 11 September 2026, and ENISA's Single Reporting Platform became operational on the same date.	verified	enisa2026faq, europeancom2026timeline, europeancyb2024reporting
CLAIM-2026-09-29-08	Regulation (EU) 2024/2847 entered into force on 10 December 2024 and its main obligations, including the essential cybersecurity requirements of Annex I, apply from 11 December 2027.	verified	europeancom2026timeline, europeancyb2024reporting
CLAIM-2026-09-29-09	CRA Annex I, Part I, point (2) requires products with digital elements to be designed, developed and produced to limit attack surfaces including external interfaces, and to ensure that vulnerabilities can be addressed through security updates including automatic updates where applicable. Subpoint letters are not asserted: the archived rendering carries proposal-era lettering.	verified	europeancyb2024annex
CLAIM-2026-09-29-10	CRA Article 13(8) requires manufacturers to ensure that vulnerabilities of a product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements in Part II of Annex I for the duration of the support period; Article 13(9) requires each security update issued during the support period to remain available for at least ten years or the remainder of the support period, whichever is longer.	verified	europeancyb2024article
CLAIM-2026-09-29-11	CVE-2026-22812 and CVE-2026-22813 are distinct, earlier OpenCode vulnerabilities - an unauthenticated HTTP server allowing arbitrary command execution, and command execution via XSS in the OpenCode web UI - with GitHub advisories GHSA-vxw4-wv6m-9hhh and GHSA-c83v-7274-4vgp published on 12 January 2026, the XSS issue affecting releases before 1.1.10.	verified	githubsecur2026crosssite

Only claims marked **verified** may carry a post. **single-source** may appear as hedged context; **disputed** must not be published at all.

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.

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.

Reporting obligations of manufacturers — CRA Article 14

PRIMARY

Publisher	European Cyber Resilience Act text
Published	2024-12-10
Retrieved	2026-09-29
Cite key	europeancyb2024reporting
URL	https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_14.html

Full text not archived — discovery/headline reference only.

Article 13 — Obligations of manufacturers (Cyber Resilience Act)

SECONDARY

Publisher	European Cyber Resilience Act
Published	2024-11-20
Retrieved	2026-09-29
Cite key	europeancyb2024article
URL	https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Article_13.html

Article 13 — Obligations of manufacturers (Cyber Resilience Act)

Regulation (EU) 2024/2847. Quoted paragraphs relevant to this edition:

Article 13(7). "The manufacturers shall systematically document, in a manner that is proportionate to the nature and the cybersecurity risks, relevant cybersecurity aspects concerning the products with digital elements, including vulnerabilities of which they become aware and any relevant information provided by third parties, and shall, where applicable, update the cybersecurity risk assessment of the products."

Article 13(8). "Manufacturers shall ensure, when placing a product with digital elements on the market, and for the support period, that vulnerabilities of that product, including its components, are handled effectively and in accordance with the essential cybersecurity requirements set out in Part II of Annex I." The support period is determined by expected product lifespan, with a minimum of five years; manufacturers must maintain coordinated vulnerability disclosure policies and appropriate policies and procedures to address vulnerabilities from internal or external sources.

Article 13(9). "Manufacturers shall ensure that each security update, as referred to in Part II, point (8), of Annex I, which has been made available to users during the support period, remains available after it has been issued for a minimum of 10 years or for the remainder of the support period, whichever is longer."

Note recorded at archive time: this paragraph set does NOT contain a requirement that updates be automatic, installed by default, or free of charge. Those sit in Annex I.

Annex I — Essential cybersecurity requirements (Cyber Resilience Act)

SECONDARY

Publisher	European Cyber Resilience Act
Published	2024-11-20
Retrieved	2026-09-29
Cite key	europeancyb2024annex
URL	https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Annex_1.html

Annex I — Essential cybersecurity requirements (Cyber Resilience Act)

Regulation (EU) 2024/2847, Annex I. Part I, point (2), subpoints as rendered by the annotated text retrieved 29 September 2026:

(a) "secure by default configuration, including the possibility to reset the product to its original state" (b) "protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems" (c) confidentiality of stored, transmitted or processed data, by encrypting relevant data at rest or in transit (d) integrity of stored, transmitted or processed data against manipulation or modification not authorised by the user (e) "process only data ... that are adequate, relevant and limited to what is necessary in relation to the intended use" (f) availability of essential functions, including resilience against and mitigation of denial-of-service attacks (g) minimise negative impact on the availability of services provided by other devices or networks (h) "designed, developed and produced to limit attack surfaces, including external interfaces" (i) reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques (j) provide security-related information by recording and/or monitoring relevant internal activity (k) "ensure that vulnerabilities can be addressed through security updates, including ... automatic updates"

Part II covers vulnerability handling: software bill of materials documentation, timely remediation, regular security testing, public disclosure of fixed vulnerabilities, a coordinated disclosure policy, vulnerability reporting mechanisms, secure update distribution, and (point 8) dissemination of patches without delay and free of charge, with advisory messages to users.

ARCHIVE CAVEAT, recorded deliberately: the page retrieved carries the 15.9.2022 proposal lettering. The subpoint LETTERS were therefore not verified against the Official Journal text of Regulation (EU) 2024/2847, and no subpoint letter is asserted in the published edition — only the Part and point, plus the substance quoted above. Verify

letters against EUR-Lex before citing them anywhere.

FAQ — CRA Single Reporting Platform

PRIMARY

Publisher	ENISA
Published	2026-09-11
Retrieved	2026-09-29
Cite key	enisa2026faq
URL	https://www.enisa.europa.eu/topics/product-security/single-reporting-platform-srp/frequently-asked-questions

Full text not archived — discovery/headline reference only.

Timeline and scope — the Cyber Resilience Act

PRIMARY

Publisher	European Commission
Published	2026-07-31
Retrieved	2026-09-29
Cite key	europeancom2026timeline
URL	https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Full text not archived — discovery/headline reference only.