Node.js Brotli decoder out-of-bounds write enabling remote code execution (CVE-2026-111497)

Status: Recovering / monitoring

Started Nov 28, 2026, 11:31 AM PST · Node.js's estimate: Fixed versions are available

CVE-2026-111497, CVE-2026-105482, CVE-2026-105483, CVE-2026-106069 · CVSS 9.2 (critical) · Being exploited: yes · Fix available: yes

WHAT'S HAPPENING

On October 21, 2026, the Node.js project released security updates fixing several flaws. The most serious, CVE-2026-111497, is in Brotli, a compression format used to shrink web data. According to the Node.js advisory, specially crafted Brotli data can make the decoder write past the end of its memory buffer. That can cause a crash, leak memory contents, or let an attacker run their own code. The score of 9.2 (critical) is a CVSS 4.0 score reported from the CVE record by secondary sources. Node.js itself rates the flaw "high". The same update also fixes a flaw that lets a server certificate pass hostname checks when it should not (CVE-2026-106069, rated high by Node.js). The advisory I opened covers the Brotli flaw and CVE-2026-106069. I did not confirm details of CVE-2026-105482 and CVE-2026-105483 from a primary source. Cisco has also published an advisory about its own products affected by these Node.js and Brotli issues. I did not open that page, so check it if you use Cisco products.

WHO IS AFFECTED

- Node.js 22.x before 22.23.4
- Node.js 24.x before 24.22.1
- Node.js 26.x before 26.12.1
- Older Node.js lines that are no longer supported (such as 25.x, 23.x and 20.x and earlier). Node.js says these are always treated as affected, and they will not get a fix.
- Applications are most exposed when they decompress Brotli data from untrusted sources. Security researchers say this includes web requests fetched with Node's built-in fetch() and request bodies handled by Express 5. A basic Node.js web server does not decode Brotli on its own.
- Other software that bundles Google's Brotli library (versions 1.0.3 through 1.2.0) may also be affected. Examples reported include Python Brotli packages, Bun, Envoy and .NET. Check each vendor's own advisory.

IS IT BEING EXPLOITED?

CISA added CVE-2026-111497 to its Known Exploited Vulnerabilities list on October 27, 2026, citing evidence of active exploitation, with a November 10, 2026 deadline for US federal agencies. Security press reports describe the first exploit attempts on October 26, 2026. CISA has not said who is exploiting it. I could not open CISA's own catalog page myself, so these details come from news and security-vendor reports.

WHAT YOU SHOULD DO NOW

Home users

- Most home users do not run Node.js directly. If you never installed it or use developer tools, you probably have nothing to do beyond keeping your devices and apps updated.
- If you installed Node.js yourself, download the latest version of your line (22, 24 or 26) from nodejs.org and install it over the old one. Then restart any programs that use it.
- If you use apps or home-server software built on Node.js (for example a self-hosted media or smart-home tool), install the app's latest update. Check the app's release notes for a Node.js or Brotli fix.
- If you are on Node.js 25, 23, 20 or older, move to a supported version. These versions will not receive a fix.

Questions? Contact BIS Computer Solutions, Inc.

5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com

Businesses

- Make a list of everything that runs Node.js: web servers, APIs, build tools, desktop apps and containers. Ask your software vendors and IT provider which versions they use.
- Update to Node.js 22.23.4, 24.22.1 or 26.12.1, or a newer release in the same line. Then restart the services. Rebuild and redeploy container images, because older images keep the old Node.js inside them.
- Treat internet-facing services that accept or fetch compressed data as the first priority.
- Move any systems on unsupported lines (25.x, 23.x, 20.x and earlier) to a supported line. These will not be patched.
- Also update other software that bundles Brotli (Python Brotli packages, Bun, Envoy, .NET and similar), following each vendor's advisory.
- Check for signs of compromise on exposed servers that were running an unpatched version after October 26, 2026. Look for unexpected crashes, restarts, new processes or unfamiliar outbound connections. If you suspect a problem, involve your IT provider or an incident-response specialist.
- Do not rely on the bundled Brotli version number to tell if a server is patched. A security vendor reports that Node.js applied the fix without changing the Brotli version string, so it reads the same on patched and unpatched builds.

HOW TO CHECK IF YOU'RE AFFECTED

- Open a command prompt (Windows) or Terminal (Mac/Linux) and run: node --version
- Compare the result with the fixed versions: v22.23.4 or later in the 22 line, v24.22.1 or later in the 24 line, or v26.12.1 or later in the 26 line.
- For containers, run the same command inside the container, for example: docker exec <container> node --version
- Do not use the Brotli version shown by process.versions.brotli. It can read the same on patched and unpatched builds.
- If you cannot check yourself, ask your IT provider or the vendor of any Node.js-based software.

FIXED VERSIONS AND WORKAROUNDS

- Node.js 22.x: 22.23.4
- Node.js 24.x: 24.22.1
- Node.js 26.x: 26.12.1
- Node.js 25.x, 23.x, 20.x and older (end of life): No fix. Move to a supported line.
- Google Brotli library (reported by security vendors): 1.0.10, 1.1.1 or 1.2.1

Until you can update:

- Node.js has not published an official workaround. The reliable fix is to update.
- If you cannot update right away, security vendor Rapid7 suggests limiting or disabling any application feature that decompresses Brotli data from untrusted sources. This is only a temporary way to reduce exposure.

OFFICIAL SOURCES

Node.js — Wednesday, October 21, 2026 Security Releases — https://nodejs.org/en/blog/vulnerability/october-2026-security-releases

OTHER COVERAGE

Rapid7: CVE-2026-111497: Critical out-of-bounds write in the Node.js Brotli decoder — https://www.rapid7.com/blog/post/etr-cve-2026-111497-critical-out-of-bounds-write-in-the-node-js-brotli-decoder/

Akamai: Inside Node2Shell: A Closer Look at CVE-2026-111497 — https://www.akamai.com/blog/security-research/inside-node2shell-closer-look-cve-2026-111497

Qualys: Node.js Patches Brotli Remote Code Execution Flaw — https://blog.qualys.com/product-tech/2026/10/23/node-js-patches-brotli-remote-code-execution-flaw-find-vulnerable-runtimes-before-attackers-do

IANS: CISA Adds Exploited Brotli Decoder Flaw to KEV — https://www.ians.com/news/cisa-flags-actively-exploited-brotli-flaw-with-broad-software-reach

SQ Magazine: CISA Adds Exploited Brotli Node2Shell Flaw to KEV Catalog — https://sqmagazine.co.uk/cisa-confirms-exploiting-brotli-node2shell-flaw/

ABOUT THIS BRIEF

Last updated November 28, 2026. Researched with AI help from public sources and checked against the official advisories above. Details can change; follow your vendor's guidance.

Questions? Contact BIS Computer Solutions, Inc.

5500 Alta Canyada Rd., La Canada, CA 91011 USA · Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com