Vulnerability Advisory

TLP: CLEAR

CAL-CSIC-2026-10-A-028

28 OCT 2026

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Out-of-Bounds Write Vulnerability in Google Brotli Decoder

Remote Code Execution	Untrusted Input Required	Under Active Exploitation	Fixed Releases Available

The Cal-CSIC has become aware of an out-of-bounds write vulnerability, CVE-2026-111497, in the Google Brotli decoder. Brotli is a compression library used by applications to decode data; processing untrusted streams can put application memory at risk. Google's CVE record rates the flaw Critical with a CVSS 4.0 score of 9.2.[1,2]

An invalid block switch in a crafted Brotli stream can be mistaken for a request for more input, causing the streaming decoder to overrun an internal buffer. The attacker must reach an application path that decompresses the stream; the flaw itself needs no credentials or user action. Successful exploitation could let the attacker crash the process, disclose its memory, or potentially execute arbitrary code. The effect depends on the application's execution context.[1,3]

Google released the fixed Brotli versions listed below, while Node.js patched its supported 22.x, 24.x, and 26.x lines. Other products bundling a vulnerable decoder require product-specific remediation. CISA added the CVE to its Known Exploited Vulnerabilities catalog on 27 October 2026, reflecting known exploitation without publishing campaign details. As of 28 October 2026, public proof-of-concept (PoC) code is available, and open-source research has demonstrated code execution in specific Node.js laboratory setups. The same research observed an apparent exploit attempt on 26 October 2026, but the captured payload did not produce a shell when reproduced.[1,3,4,5]

The Cal-CSIC recommends that clients identify applications and services decoding untrusted Brotli data, prioritizing internet-facing systems and bundled copies. Upgrade direct Brotli installations to the fixed release for their branch, and apply relevant vendor updates to runtimes, packages, and appliances. If updating is delayed, restrict or disable decoding of untrusted Brotli data where feasible. Review recent crashes and anomalous activity on exposed systems and investigate suspicious findings.[1,3,6]

For additional details regarding CVE-2026-111497, please use this link:

Google Brotli Security Releases:

https://github.com/google/brotli/releases

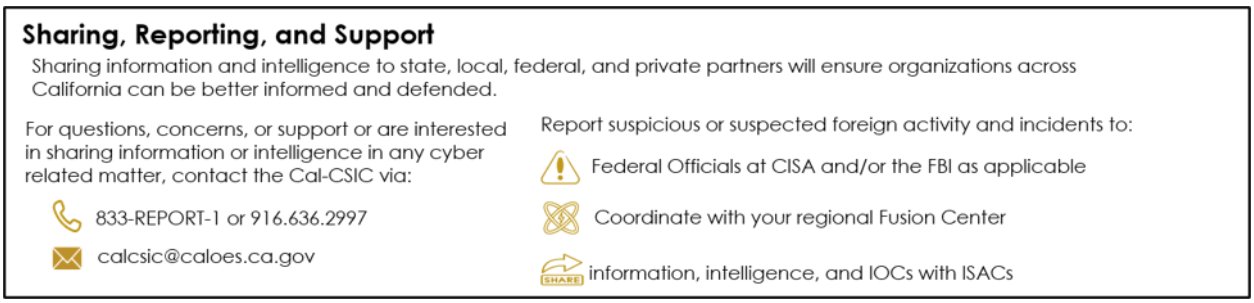
WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Affected Products and Versions

Product	Affected Version	Fixed Release
Google Brotli 1.0.x	1.0.3 to before 1.0.10	1.0.10
Google Brotli 1.1.x	1.1.0 to before 1.1.1	1.1.1
Google Brotli 1.2.x	1.2.0 to before 1.2.1	1.2.1

These are upstream Google Brotli ranges. Bundled or backported copies require product-specific verification; an upstream version string alone may not show whether a vendor fix is present.[1,6]

Sharing, Reporting, and Support



References

[1] Google (CVE Program); "CVE-2026-111497: Out-of-Bounds Write in Google Brotli Decoder"; https://raw.githubusercontent.com/CVEProject/cvelistV5/main/cves/2026/111xxx/CVE-2026-111497.json; accessed 28 October 2026

[2] Google; "Brotli compression format"; https://github.com/google/brotli; accessed 28 October 2026

[3] Node.js Project; "Wednesday, October 21, 2026 Security Releases"; https://nodejs.org/en/blog/vulnerability/october-2026-security-releases; accessed 28 October 2026

[4] Cybersecurity and Infrastructure Security Agency; "Catalog of Known Exploited Vulnerabilities"; https://raw.githubusercontent.com/cisagov/kev-data/develop/known_exploited_vulnerabilities.json; accessed 28 October 2026

[5] ELLIO Threat Research Lab; "Node2Shell: remote code execution on stock Node.js builds (CVE-2026-111497)"; https://ellio.tech/en/blog/node2shell-cve-2026-111497-rce-on-stock-nodejs-builds/; accessed 28 October 2026

[6] Red Hat; "CVE-2026-111497"; https://access.redhat.com/security/cve/cve-2026-111497; accessed 28 October 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.