Google Brotli Security Bulletin

Date: October 29, 2026

Version: 1.0

Summary

VIAVI Solutions is aware of the recently disclosed Google Brotli decoder vulnerability, CVE-2026-111497, also known as Brotli2Shell, Node2Shell, HTTP2Shell, and Broccoli2Shell, and is assessing potential impact across applicable NSE product .

This is not a vulnerability in VIAVI software, but may affect products or components that include or depend on a vulnerable version of the Brotli open-source library. Fixed Brotli releases are available, and CISA added the vulnerability to its Known Exploited Vulnerabilities (KEV) catalog on October 27, 2026.

The assessment is ongoing. Additional information regarding product impact and recommended mitigation, if required, will be published as it becomes available. VIAVI is not currently aware of any exploitation of VIAVI products related to this vulnerability.

Vulnerability Details

CVE-2026-111497 is an out-of-bounds write in the Google Brotli decoder (C library). An application that decompresses crafted Brotli data can suffer memory corruption, which may lead to information disclosure, denial of service, or remote code execution. The flaw can be triggered in both directions: a malicious client can attack a vulnerable server, and a malicious server can attack a vulnerable client that accepts compressed responses. Public proof-of-concept exploits are available.

The vulnerability affects Brotli versions 1.0.3 through 1.2.0 and is fixed in 1.0.10, 1.1.1, and 1.2.1, released on October 21, 2026. Google scored it 9.2 (Critical) under CVSS v4.0; Red Hat rates it 8.1 under CVSS v3.1. The fix was committed upstream in February 2026 but was not released until October. Affected software includes Node.js, .NET, Bun, Envoy Proxy, Istio, Python Brotli packages, PHP for Windows, and Firefox, as well as any application that bundles its own copy of the library. A security firm reported observing an exploitation attempt on its sensor network on October 26, and CISA added the vulnerability to its catalog on October 27 with a remediation due date of November 10 for U.S. federal agencies. Recommended action is to update to patched versions of affected runtimes and libraries, including bundled copies, and to restrict Brotli decompression of untrusted input where updates are not yet possible.

References

https://www.tenable.com/blog/brotli2shell-frequently-asked-questions-for-google-brotli-decoder-cve-2026-111497

https://access.redhat.com/security/vulnerabilities/RHSB-2026-015

https://www.bleepingcomputer.com/news/microsoft/microsoft-releases-emergency-net-patches-for-critical-brotli-flaw/