

CVE-2026-111497

Microsoft Google: CVE-2026-111497 Buffer overflow vulnerability in the Brotli decoder

A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. Users need to update any Brotli libraries or binaries between 1.0.3 through 1.2.0 to the latest available version: 1.0.10 or 1.1.1 or 1.2.1.

EVRS 24 /100 Elevated priority	CVSS V4.0 9.2 Critical · NVD	EPSS 0.328 98.3rd percentile · FIRST	CISA DEADLINE — No CISA deadline
---	---	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 3 of 8 signals

☐ CISA KEV	Not currently CISA KEV-listed	☐ Vendor exploitation	Active-exploitation status not yet checked - scored at the population base rate (none) until known
☐ Ransomware	Ransomware association unavailable	☐ KEV recency	CISA KEV listing date unavailable
☒ EPSS	0.328 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Scheduled Maintenance Patch or fixed version identified
Basis: External remediation intelligence

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
Not identified by the connected sources	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-9v8h-qqgm-4m35
ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2026-108169

NVD nvd.nist.gov/vuln/detail/CVE-2026-111497
Current data evulnable.com/vulnerability-management/cve/CVE-2026-111497

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.