VIVOTEK
A Delta Group Company

VIVOTEK Product Security Advisory

Advisory ID: VVTK-SA-2026-07

CVE ID: CVE-2026-111497

First Published: November 5th , 2026
Last Update: November 5t, 2026
Status: Confirmed
Revision: 1.0

Executive Summary

Google Brotli Decoder Vulnerability

A critical out-of-bounds write vulnerability (CVE-2026-111497; CWE-787 / CWE-252) has been disclosed in the Google Brotli compression decoder (c/dec/decode.c). When an application decompresses an untrusted or malformed Brotli-compressed data stream (such as via HTTP Content-Encoding: br, Node.js node:zlib, .NET runtime, or media decoders like FFmpeg via libjxl), an attacker could potentially induce memory corruption, application crash, or remote code execution (RCE).

VIVOTEK has conducted a comprehensive security assessment across all product lines, firmware builds, and cloud backend stacks:

- **VEX Status - Known Not Affected:** All VIVOTEK products, firmwares, and services are officially confirmed as known_not_affected.
- **VAST Security Station (VSS) & NVRs (NR9581-V3, NR9682-V3, VNR032A-08, VNR064A-16):** While FFmpeg 7.1.5 is utilized for multimedia streaming, VIVOTEK builds FFmpeg with custom CMake rules (codec-selection.cmake) that disable all decoders (--disable-decoders) and strictly whitelist only surveillance-essential formats (H.264, HEVC, MJPEG, MPEG4, audio). The libjxl (JPEG XL) decoder is completely absent (component_not_present), neutralizing the reported attack vector.
- **VORTEX AI & VPP Cloud Backends:** Although underlying runtime environments (.NET runtime in HMC-Backend, Go package andybalholm/brotli in VPP-Backend, and shared libraries in VORTEX AI) contain Brotli code, rigorous code audit confirms the vulnerable decoder functions are never invoked nor reachable by adversary input (vulnerable_code_not_in_execute_path / vulnerable_code_cannot_be_controlled_by_adversary).

VIVOTEK
A Delta Group Company

Security Evaluation Conclusion: No attack surface exists within VIVOTEK solutions for CVE-2026-111497. Customers, security integrators, and system administrators do not need to apply emergency hotfixes, alter network configurations, or disable core surveillance operations.

Overview:

Vulnerability ID	CVE-2026-111497 (Google Brotli Decoder Out-of-Bounds Write)
Common Weakness Enumeration	CWE-787: Out-of-bounds Write | CWE-252: Unchecked Return Value
Affected Third-Party Components	Google Brotli decoder (c/dec/decode.c v1.0.3-1.2.0), bundled .NET Core runtime (< 10.0.14), Go andybalholm/brotli (< v1.2.7), FFmpeg with libjxl
Trigger Condition	Decompressing untrusted Brotli payloads: HTTP Content-Encoding: br, fetch()/curl auto-decompression, or JPEG XL image decoding
Exploitability in VIVOTEK	None. No product accepts and decompresses external untrusted Brotli data. Vulnerable paths are either compiled out or excluded from execution flows.

Affected Products:

Product Line / Model	Software Ver.	Component	Vulnerability Analysis & Technical Justification	VEX Status
VAST Security Station (VSS) (Standalone Software)	v1.6.0.2020	FFmpeg 7.1.5	Not Affected (component_not_present): Custom codec-selection.cmake disables all decoders and whitelists only surveillance codecs. libjxl/JPEG XL is not enabled.	known_not_affected
NR-Series NVRs (NR9581-V3, NR9682-V3)	VSS v1.6.0.2020	FFmpeg 7.1.5	Not Affected (component_not_present): Same custom build flags; neither libjxl nor JPEG XL decoders are compiled into the binary.	known_not_affected
VNR-Series NVRs (VNR032A-08, VNR064A-16)	VSS v1.6.0.2020	FFmpeg 7.1.5	Not Affected (component_not_present): Built without libjxl/JPEG XL decoders. Attack vector cannot be reached.	known_not_affected
VORTEX AI	v6.4.34.1	Brotli 1.2.0	Not Exploitable (vulnerable_code_not_in_execute_path): Cannot be triggered in any supported deployment configuration. Routine upgrade to v6.4.34.2 (2026-11-05).	known_not_affected
VPP Portal (HMC-Backend)	v1.3.0.0	.NET Runtime 10.0.10	Not Exploitable (vulnerable_code_not_in_execute_path): Only uses ResponseCompression; no request decompression configured. Rebuild to v1.3.1.0 on 2026-11-18.	known_not_affected
VPP Portal (VPP-Backend)	v1.3.0	Go andybalholm/brotli v1.2.1	Not Exploitable (vulnerable_code_cannot_be_controlled_by_adversary):	known_not_affected

Indirectly pulled by ClickHouse driver; application only uses PostgreSQL. Rebuild to v1.4.2 on 2026-11-18.

Workaround:

Although VIVOTEK products are not affected by this vulnerability, standard surveillance cybersecurity best practices are recommended:

- Network Segmentation: Maintain surveillance devices, NVR appliances, and management platforms within isolated surveillance VLANs segregated from public and unauthenticated networks.
- Web Gateway & Reverse Proxy Hygiene: Where reverse proxies or WAFs front web endpoints, enforce standard vendor-recommended payload inspection and compression validation baselines.
- Routine Maintenance: Maintain systems on regular software and firmware release cycles to benefit from continuous security hardening.

Solution:

Action Required by Customers: None. System administrators, partners, and customers do not need to take any remediative action or apply emergency hotfixes.

Scheduled Platform Maintenance: To maintain defense-in-depth and software hygiene, VIVOTEK development teams have scheduled routine runtime rebuilds across cloud backends with zero service disruption.

Revision History:

Revision	Date	Description
1.0	November 5, 2026	Initial release