CYBERSECURITY RISK ADVISORY

HTTP2Shell: Exploited Flaw in the Brotli Compression Library Behind Node.js, .NET, Python and More (CVE-2026-111497)

All sectors · Development, platform and infrastructure teams · Any organization running web services, APIs, proxies or appliances that decompress Brotli data

ADVISORY ID	PUBLISHED	CLASSIFICATION	SEVERITY
SCA-ADV-2026-003	November 17, 2026 · v1.0	TLP:CLEAR	Critical

STATUS

Actively exploited · in CISA KEV

Developing situation. This advisory reflects public information as of **November 17, 2026, 12:00 PM Eastern Time**. Vendors are still releasing fixes for products that bundle Brotli, so check your vendors' advisories before acting. Each fact carries a numbered citation [1] that links to its source in Appendix A, and claims are attributed to the organization that made them. We deliberately leave out exploit details. TLP:CLEAR means this advisory may be shared without restriction.[11]

1. Executive summary

CVE-2026-111497, nicknamed **HTTP2Shell** (also Node2Shell or Broccoli2Shell), is an out-of-bounds write in the decoder of **Brotli**, Google's widely used compression library. A specially crafted compressed stream can crash a program, leak its memory or, in some cases, let an attacker run code, without logging in.[2] [6] Google rates it **9.2 (Critical) under CVSS v4.0**.[1] Despite the name, it is not an HTTP/2 flaw: any software that decompresses Brotli data from an untrusted source can be exposed, including Node.js, .NET, PowerShell, Bun, Python HTTP clients, Envoy and Istio.[2] [6] CISA added it to its Known Exploited Vulnerabilities (KEV) catalog on October 27, 2026, and urged all defenders, not only federal agencies, to prioritize patching.[3] [10]

Bottom line for executives

- **This hides inside other software.** Brotli is bundled into runtimes, proxies, appliances and packages, so the question is not "do we use Brotli?" but "which of our products decompress it?" Ask your developers and vendors.[2] [5]
- **Update and restart.** Fixed releases exist for the Brotli library (1.2.1, 1.1.1, 1.0.10), Node.js (22.23.4, 24.22.1, 26.12.1), .NET, PowerShell, Bun, Python packages, Envoy and Istio. Running programs and container images keep the old code until they are restarted or rebuilt.[1]
- **If you can't patch yet,** stop affected applications from decompressing Brotli data from untrusted sources, for example by rejecting Brotli-encoded requests at the proxy.[1] [2]
- **Unsupported versions stay vulnerable.** Node.js 20.x, 23.x and 25.x will get no fix; move to a supported line.[5]

2. What happened

WHEN (2026)	EVENT	SOURCE
Feb 27	A fix was committed to Google's Brotli repository with no release or advisory. It stayed publicly readable for about eight months.	[1] [5]
Oct 21	Node.js disclosed the flaw and released 22.23.4, 24.22.1 and 26.12.1; Brotli 1.2.1, 1.1.1 and 1.0.10 were released. Researchers at OpenAI reported the bug.	[1] [5]
Oct 22	The CVE was published. Imperva demonstrated code execution against the official Node.js 24.22.0 Linux arm64 image, after multiple attempts. Bun 1.4.4 was released.	[1] [5]
Oct 25	Microsoft released out-of-band .NET updates.	[1] [10]
Oct 26	PHP rebuilt its official Windows packages (8.5.12-1, 8.4.27-1, 8.3.36-1, 8.2.35-1) with Brotli 1.2.1. Threat intelligence firm ELLIO recorded exploit traffic in the wild.	[5] [7] [14]
Oct 27	CISA added CVE-2026-111497 to the KEV catalog, with a federal due date of November 10, and said it had confirmed exploitation in the wild without naming targets.	[1] [3] [10]
Oct 28	The Canadian Centre for Cyber Security issued Alert AL26-027.	[2]
Nov 2–12	Arista published Advisory 0202 for its VeloCloud Orchestrator and, on November 12, added VeloCloud Edge and DMF Analytics Node.	[8]

3. The vulnerability

When the decoder misreads an invalid part of a compressed stream, it keeps appending data to a small internal buffer and writes past its end, corrupting nearby memory.[6]

CVE	WHAT GOES WRONG	SEVERITY	ACCESS NEEDED	IMPACT
CVE-2026-111497	Out-of-bounds write (CWE-787) in the Brotli decoder, versions 1.0.3 through 1.0.9, 1.1.0 and 1.2.0[2] [6]	CVSS v4.0 9.2	None: the attacker only needs to get crafted compressed data to a program that decompresses it[2]	Crash, memory disclosure, possible remote code execution[2]

- **Both directions:** a server or proxy that decompresses Brotli-encoded requests can be attacked by a malicious client, and a client that automatically decompresses responses can be attacked by a malicious or compromised server.[1] [8]
- **Ratings vary by product:** Node.js rates it High, Microsoft rates .NET at CVSS v3.1 8.1, and Arista rates its products at CVSS v3.1 9.8.[1] [8]
- **Not every installation is exposed.** In .NET, Brotli decompression is off by default; Envoy and Istio are affected only if their Brotli decompressor is enabled; curl decodes Brotli only when asked to.[1] In PHP's Windows packages, the flaw is reachable through the cURL extension when automatic decompression is turned on. According to The Hacker News, the Guzzle HTTP client turns it on by default, though the publication says it did not test this on Windows.[7]
- **Other software named by researchers:** Tenable also lists FFmpeg, Apache Arrow and ClickHouse.[5] Broadcom says SDDC Manager in VMware Cloud Foundation is affected through its bundled Node.js runtime and points to advisory VMSA-2026-0008, and Palo Alto Networks has published its own advisory.[9] [13]

4. Affected and fixed versions

PRODUCT	FIXED IN	NOTES
Google Brotli library	1.2.1 · 1.1.1 · 1.0.10	Affected: 1.0.3–1.0.9, 1.1.0, 1.2.0[2]
Node.js	22.23.4 · 24.22.1 · 26.12.1	20.x, 23.x and 25.x are end of life and get no fix[1] [5]
Bun	1.4.4	Rebuild standalone binaries[1]
.NET runtime	8.0.33 · 9.0.22 · 10.0.14	.NET Framework not affected; rebuild self-contained apps[1]

PRODUCT	FIXED IN	NOTES
PowerShell	`7.4.22 · 7.5.13 · 7.6.9`	[1]
Python `brotli` / `brotlicffi`	`1.2.1 · 1.2.1.0`	Used automatically by requests, httpx and aiohttp when installed[1]
Envoy	`1.40.0 · 1.39.3 · 1.38.6 · 1.37.8 · 1.36.12`	Only if the Brotli decompressor is enabled[1]
Istio	`1.31.2 · 1.30.6 · 1.29.9`	Only if the Brotli decompressor is enabled[1]
PHP for Windows (php.net builds)	`8.5.12-1 · 8.4.27-1 · 8.3.36-1 · 8.2.35-1`	`php -v` shows the same version before and after; check the -1 build suffix[7]
Arista VeloCloud Orchestrator	`5.2.3.20 · 6.1.3.12 · 6.4.2.14`	No workaround[8]
Arista VeloCloud Edge	`7.0.1.1 · 6.4.4.2 · 6.1.6.2 · 5.2.7.2`	No workaround[8]
Linux distributions	Vendor packages	Debian and Red Hat have shipped fixed brotli packages; check your distribution's advisory[1]

Other bindings: Java brotli4j is fixed in 1.24.0 and the Ruby brotli gem in 0.9.1; Go's cbrotli needs a patched system library.[1] For appliances and commercial products, follow the vendor's advisory.

5. Exploitation and exposure

- **CISA's KEV catalog:** CISA added CVE-2026-111497 on October 27, 2026, with a federal due date of November 10. It gave no details about the attacks.[3] [10]
- **Activity seen by researchers:** ELLIO told Help Net Security that its sensors recorded exploit traffic in the wild "carrying the public exploit" that ELLIO had confirmed gets a shell on vulnerable builds, from an address it had previously seen carrying PHP2Shell exploits, probing VPNs and scanning Kubernetes APIs. ELLIO called this "indicative of the RCE being adopted by an operator focused on mass exploitation."[5] In its own write-up, ELLIO dates that traffic to October 26 and says the attack chain it captured produced no shell in 50 attempts against a vulnerable Node.js 24.22.0 target; it calls this likely a first-generation attempt and reports no confirmed compromise.[14]
- **Mixed evidence of success:** SecurityWeek reports that two security firms recorded exploitation attempts against honeypots.[4] CISA has confirmed exploitation but has not described the attacks.[10] Treat exploitation as real, but its success rate as unknown.

- **Public exploit code:** proof-of-concept exploits are on GitHub.[5]
- **Vendor reports:** Microsoft reported no exploitation as of October 25, and Arista's advisory does not report any exploitation of its products.[1] [8]

9.2	~8 months	Nov 10
CVSS v4.0 score assigned by Google[1]	the fix sat public in Brotli's code before a release[5]	CISA's deadline for U.S. federal agencies[3]

6. Business risk

- **Code execution in your services:** a successful attack runs code inside the affected process, which may hold API keys, database credentials or customer data. In containers, that can expose service-account tokens and cloud credentials.
- **Outbound calls are a path in:** applications that fetch content from user-supplied or partner URLs can be attacked by whoever controls the other end.[1] [8]
- **Long tail:** Brotli is embedded in many products, and Linux distributions and downstream vendors are releasing fixes on their own schedules; Arista, for example, had no patch for its DMF Analytics Node when it updated its advisory.[5] [8] Unpatched appliances and old container images are the likely gaps.
- **Availability:** even where code execution is hard, crafted data can crash services.[2]

7. Recommended actions

Today

1. **Inventory** Brotli across hosts, container images, dependencies and vendor products, starting with internet-facing systems.[2] Check versions directly (for example `node -v`, `pip show brotli brotlicffi`) rather than relying on external scans.[1]
2. **Update** to the fixed versions in Section 4, then **restart services and rebuild container images** so the new code actually runs.[1] [5]
3. **If you can't update yet,** reject `Content-Encoding: br` at the proxy or load balancer, or turn off request decompression in body parsers. Neither stops a client from decoding a malicious response, so also stop decoding Brotli from untrusted sources.[1] [2]
4. **Ask your vendors**, especially for appliances, SD-WAN, proxies and virtualization management, whether their products bundle a vulnerable Brotli and when fixes ship.[4] [8]

Within 72 hours

1. **Prioritize services that decompress untrusted data:** Node.js apps using Express 5, body-parser 2.x, Koa body parsers or @fastify/compress with request decompression, and any code that fetches user-supplied URLs.[1]
2. **Replace end-of-life runtimes** such as Node.js 20.x.[1] [5]
3. **Watch for crashes** and abnormal process behavior in services that handle compressed data.[2]
4. **If you find signs of compromise,** rotate credentials the affected process could read and treat it as an incident.

Strategic

1. **Keep a software bill of materials** for applications and images, so a library flaw can be scoped in hours.
2. **Rebuild images on a schedule,** not only when code changes.
3. **Track CISA's KEV catalog** and set patch deadlines for exploited flaws.[3]

8. What to watch for

- Unexpected crashes or restarts of services that decompress data.[2]

- Brotli-encoded requests (`Content-Encoding: br`) to APIs that don't normally receive them; a reverse proxy or WAF can see this header. Datadog calls an edge rule that rejects Brotli-compressed request bodies "a useful tripwire and nothing more," and notes that body-size limits don't help.[12]
- Node.js, Python or .NET processes starting shells or making unexpected outbound connections.[12]

9. Questions for leadership

1. Which of our applications, images and vendor products include Brotli, and who owns each one?
2. Are our internet-facing services on fixed versions, and have they been restarted or rebuilt?
3. Which vendors have confirmed their products are fixed, and which have not answered?
4. Are we still running end-of-life runtimes that will never get this fix?

Appendix A. Source map

Every citation, traced to its publisher. Sources were opened and checked on November 17, 2026, and independently fact-checked before publication, except where noted.

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
1	Discovery by OpenAI; Feb 27 fix commit; CVSS v4.0 9.2 (Google), Node.js High, Microsoft CVSS v3.1 8.1; timeline Oct 21–27; fixed versions for Brotli, Node.js, Bun, Python, .NET, PowerShell, Envoy, Istio, Java and Ruby bindings, Go; Linux distribution packages; curl behavior; .NET off by default; Microsoft's Oct 25 no-exploitation statement; mitigations and exposure checks	Cycode (updated Oct 30, 2026)	Security vendor	cycode.com
2	Alert AL26-027 (Oct 28, 2026): vulnerability description; impacts; affected products; affected and fixed Brotli versions; inventory, patching, untrusted-content and monitoring advice	Canadian Centre for Cyber Security	Canadian government	cyber.gc.ca
3	KEV catalog version 2026.11.13, checked Nov 17 via CISA's official kev-data repository: CVE-2026-111497 added Oct 27, due Nov 10	CISA Known Exploited Vulnerabilities catalog, via official kev-data repository	U.S. government	cisa.gov · data

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
4	Two security firms recorded exploitation attempts against honeypots (based on a search summary; the page could not be loaded from our environment)	SecurityWeek	Security news	securityweek.com
5	Node.js disclosure Oct 21; ELLIO's in-the-wild traffic and quote; public PoCs; Imperva demonstration; Tenable's list of affected software; end-of-life Node.js lines; Feb 27 commit public for eight months; distributions and downstream vendors releasing fixes; rebuild and restart advice	Help Net Security, "Brotli bug reaches far beyond Node.js (CVE-2026-111497)," Oct 27, 2026 (updated Oct 28)	Security news	helpnetsecurity.com
6	Names; affected Brotli versions; how the buffer overflow happens; not specific to HTTP/2	BleepingComputer, "Critical 'HTTP2Shell' Brotli vulnerability triggers emergency patches," Oct 26, 2026	Security news	bleepingcomputer.com
7	PHP's Oct 26 rebuilt Windows packages with Brotli 1.2.1; reachable through the cURL extension with automatic decompression; Guzzle default; php -v unchanged; build suffix check	The Hacker News, "PHP Issues Second Windows Security Update in Five Days to Fix Brotli Code Execution Flaw," Oct 26, 2026	Security news	thehackernews.com
8	Security Advisory 0202 (Nov 2; rev 1.1 Nov 12): CVSS v3.1 9.8 for Arista products; VeloCloud Orchestrator and Edge affected and fixed versions; required configuration (outbound client fetching crafted responses); no workaround for Orchestrator or Edge; no patch yet for DMF Analytics Node; no exploitation reported	Arista Networks	Vendor	arista.com
9	Exploited in the wild; vendor advisories including Palo Alto Networks, Broadcom (VMware Cloud Foundation), Node.js, .NET and PHP	Hong Kong Computer Emergency Response Team (HKCERT), Oct 28, 2026 (last updated Nov 9)	Government-funded CERT	hkcert.org
10	CISA's KEV addition on Oct 27 under BOD 26-04, its confirmation of exploitation without attack details, and its call for all defenders to prioritize patching; Microsoft's Sunday (Oct 25) .NET update	BleepingComputer, "CISA warns of hackers now exploiting critical Node2Shell flaw," Oct 28, 2026	Security news	bleepingcomputer.com

#	WHAT IT SUPPORTS	SOURCE	TYPE	LINK
11	TLP:CLEAR definition; Traffic Light Protocol 2.0	FIRST	Standards body	first.org
12	Reproduction analysis; an edge rule rejecting Brotli-compressed request bodies is "a useful tripwire and nothing more"; Content-Encoding header visible to proxies; body-size limits don't help; shells and new outbound connections as signals	Datadog Security Labs, Oct 29, 2026	Security vendor	securitylabs.datadoghq.com
13	SDDC Manager in VMware Cloud Foundation affected through the Node.js Brotli decoder; remediation in VMSA-2026-0008	Broadcom knowledge base article 460791, "Node.js Brotli decoder vulnerability, CVE-2026-111497, and VMware by Broadcom product portfolio"	Vendor	knowledge.broadcom.com
14	Oct 26 in-the-wild exploit traffic; captured attack chain produced no shell in 50 attempts; public exploit confirmed to get a shell; no confirmed compromise	ELLIO, "Node2Shell: remote code execution on stock Node.js builds (CVE-2026-111497)," Oct 25, 2026 (updated with Oct 26 activity)	Threat intelligence vendor	ellio.tech

Strat Cyber Advisors · Advisory SCA-ADV-2026-003 · v1.0 · Published November 17, 2026 · **TLP:CLEAR**

This advisory summarizes public information for awareness and planning. It is not legal advice and does not replace guidance from your vendors or incident responders. Need help assessing exposure? Contact advisors@stratcyberadvisors.com.