It's Probably Nothing
by Sierra Echo Charlie

EDITION 16 / 29 OCTOBER 2026

Brotli joins the known-exploited list

Adobe's upload flaw has a crucial caveat; NT Health pauses its observer programme.

3 stories / Listen online - 2:50

THE TAKEAWAY

The Brotli follow-up is more consequential than another patch notice: CISA now has evidence of active exploitation. But the vulnerable code still has to be reachable, which is rather more useful than treating every Node.js installation as the same problem.

01 / THE BRIEF

Brotli's exploitation status changes the priority

CISA added CVE-2026-111497 to its known-exploited catalogue on 27 October. That's the new development, rather than another affected-product announcement.

Node.js says an attacker must supply Brotli data that an application decompresses with node:zlib. The resulting process-memory corruption can cause crashes, disclose memory or allow remote code execution. Having Node.js installed isn't, by itself, the whole exposure story.

Fixed Node.js releases are 22.23.4, 24.22.1 and 26.12.1. The catalogue addition doesn't establish when attacks began or how widespread they are; ransomware-campaign use remains unknown.

WORTH ASKING

If you're running a service that decompresses untrusted Brotli input, that decoding path is worth checking against the fixed releases.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

CISA Adds Two Known Exploited Vulnerabilities to Catalog - Primary source

Wednesday, October 21, 2026 Security Releases - Primary source

Node2Shell Brotli Flaw Enables Node.js Code Execution and Exposes Other Software - Reporting / context

02 / THE BRIEF

Adobe’s upload flaw is being exploited, with a caveat

The other CISA addition is CVE-2026-48356, an unrestricted-upload flaw affecting Adobe Commerce and Magento Open Source. Adobe’s July bulletin said it knew of no exploits for the issues it addressed; CISA now cites evidence of active exploitation.

There’s an important wrinkle: Adobe’s CVE-specific entry requires neither authentication nor administrator privileges, but its CVSS vector does require user interaction. CISA describes possible code execution in the current user’s context and elevated access or control over their account or session. That isn’t the same claim as an interaction-free storefront takeover.

The fixes are in July’s APSB26-73 releases, not a fresh patch drop.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

CISA Adds Two Known Exploited Vulnerabilities to Catalog - Primary source

Security update available for Adobe Commerce | APSB26-73 - Primary source

03 / THE BRIEF

NT Health pauses observers after maternity privacy breach

ABC reports that NT Health has paused its medical-observer programme following a Royal Darwin Hospital maternity privacy breach. Instagram photos and videos exposed patient names, identification numbers, medical conditions and other sensitive information.

Health Minister Steve Edgington said on Wednesday morning that he’d referred the breach to the NT Information Commissioner and NT Police to determine whether criminal offences had occurred. The referral isn’t a finding that an offence occurred.

The patient-count revision came on Tuesday: NT Health said specialist ICT assistance had unlocked previously inaccessible files, taking its acknowledged total from five to twelve. Four affected patients told ABC the department hadn’t notified them before the outlet contacted them. This wasn’t a network intrusion, but information handling and notification failures are quite capable of doing harm without one.

SOURCES

NT Health backtracks on claim only five patients impacted by RDH privacy breach - Reporting / context

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.