Weekly Cybersecurity Briefing (26 October – 1 November 2026)

CyberSecBrief Team

CyberSecBrief provides clear, concise cybersecurity briefings that summarise the most relevant developments of the week. The report highlights notable incidents, key themes, and significant activity across the threat landscape, supported by daily updates sourced from trusted feeds and advisories. Its purpose is to offer a practical, time-efficient overview for readers who need a reliable snapshot of current cybersecurity events.
For more briefings, visit CYBERSECBRIEF.COM.



November 2, 2026

Editorial Analysis

PHP2Shell and **Node2Shell** both entered CISA's Known Exploited Vulnerabilities catalogue this week. For Node2Shell, the main question is how many systems can actually be fixed. Qualys telemetry shows that only around 42,000 of approximately three million Node.js installations had been patched, while 1.7 million were running end-of-life versions that will not receive fixes. Two honeypot operators recorded exploitation attempts, one of which involved a broken exploit.

Several incidents exposed a gap between patching a product and updating the vulnerable component it actually uses. **GitLab**'s remediation for CVE-2026-97229 patches the Ruby bundled with GitLab's own packages and images. **Alpine Linux**'s upgrade to GitLab 19.3.6 therefore left its instance vulnerable because its image used the system Ruby, and the issue was discovered on 26 October. **Brotli** creates a similar complication across ecosystems. The library is bundled in Node.js and PHP's Windows builds, while vulnerable versions are also present in Python packages that advisory databases initially failed to map to CVE-2026-111497. **Oracle** addressed three PeopleSoft weaknesses under the single identifier CVE-2026-35273, prompting researchers to seek separate identifiers. In these cases a product's version number or an apparently completed upgrade did not, on its own, establish whether the affected code had been updated.

The FBI formally attributed the **Binance** theft to North Korea's TraderTraitor and published cryptocurrency addresses associated with the laundering operation. Talos assessed with high confidence that **KeyDrift**'s infrastructure overlapped with Volt Typhoon's Silent Train network, while explicitly stopping short of attributing KeyDrift itself to Volt Typhoon. AI appeared in several incidents in different roles. The **VOLTA** infostealer used language models to rank victims by the value of their stolen data, Chainalysis disclosed an intrusion involving what it called "offensive agentic techniques", and a trojanised Claude Code extension reached up to 5,000 Cursor users. These cases do not establish a single common method or threat actor.

Deep Dive: PHP2Shell, Two Weeks On

The first week of PHP2Shell reporting ended with conflicting evidence. Sophos confirmed one compromise that delivered the Potassium Mirai variant, while CrowdStrike found no exploitation in the wild or in its honeypots. WatchTowr found that much of the publicly available exploit code failed, and Amazon recorded an attempted attack on 17 October, before the vulnerability details became public.

The second week brought clearer evidence that the exploit chain could succeed, although its reliability remained uncertain. On 26 October, CISA added CVE-2026-109618 and CVE-2026-109619 to its Known Exploited Vulnerabilities catalogue, setting a 29 October remediation deadline for federal agencies without disclosing the exploitation evidence behind the decision.

© CyberSecBrief 2025—2026

On 23 October, CISA had said it had not observed successful exploitation. Perplexity researcher Adel Karimi's honeypots subsequently recorded 35 shell executions on 24 October from two IP addresses. The attacks used a four-stage request chain that leaked memory before executing a command. However, the test environment was deliberately favourable: a single-worker `mod_php` configuration running PHP 8.4.26. No second-stage payload was observed, and Wiz reported that none of the attempts it tracked succeeded. The results demonstrate that the chain can work under specific conditions, not how reliably it works across other deployments.

The strongest evidence of substantial intrusion came from attacks against firewalls. Dream reported that attackers scanned approximately 19,000 firewalls, fingerprinted around 5,000 and narrowed their targets to 240 devices in the US, Japan, Taiwan and South Korea. They obtained root access on 24 servers and later a 25th, chaining PHP2Shell with the Fragnesia Linux kernel vulnerability, which CISA had also urged federal agencies to patch. On a US government-affiliated firewall, the attackers tunnelled into the internal network, recovered a decrypted LDAP service-account password and began enumerating Active Directory. Unit 42 independently verified the attackers' tooling and reported exploitation of internet-exposed PAN-OS management interfaces. Palo Alto Networks said approximately 0.02% of its installed base was affected and that its patches break the exploit chain. Unit 42 also retracted its 23 October update after it could not link a reported intrusion involving a European government to the vulnerabilities.

Important uncertainties remain. Dream could not recover the results of later attack stages, leaving it unclear whether password spraying, backdoor account creation or SAML key extraction succeeded. No threat actor has been named. Dream cited FOFA use, UTC+8 timestamps and Chinese-language prompts as indicators of a possible Chinese nexus, not conclusive attribution. The estimate of 22.6 million potentially exposed instances measures possible exposure, not confirmed vulnerability or compromise. Bitsight also reported a surge in scanning, but few reliable exploits. Separately, for CVE-2026-115560, PHP has published mitigations rather than a patch, and the available evidence here does not indicate exploitation.

Highlights of the Week

PHP2Shell Exploitation Confirmed as Attackers Root Firewalls

CISA added PHP2Shell flaws CVE-2026-109618 and CVE-2026-109619 to its Known Exploited Vulnerabilities catalogue on 26 October, after honeypots recorded 35 shell executions on 24 October. Dream reported that suspected Chinese attackers chained the flaws with the Fragnesia Linux kernel bug to root 25 servers, including PAN-OS firewalls. Unit 42 counts more than 22.6 million potentially exposed instances.

Sources:

- CISA
- SecurityWeek
- BleepingComputer
- Dream
- Palo Alto Networks Unit 42

Brotli Node2Shell Flaw Exploited as Emergency Patches Spread

CVE-2026-111497, an out-of-bounds write in Google's Brotli decoder, was added to CISA's catalogue on 27 October after honeypots logged exploitation attempts. Microsoft issued out-of-band fixes for .NET, Visual Studio and PowerShell, and PHP rebuilt its Windows packages. Qualys telemetry shows about 42,000 of roughly three million Node.js installations patched, with 1.7 million on end-of-life versions.

Sources:

- BleepingComputer
- SecurityWeek
- The Hacker News
- Sophos

FBI Attributes Record $6 Billion Binance Theft to North Korea

Binance reported that about $6.3 billion in assets was stolen, which it linked to a compromised DevOps engineer's laptop before reporting additional points of breach. The FBI attributed the theft to North Korea's TraderTraitor and said the actors are converting stolen assets mainly into Ethereum. Binance says it will cover all losses.

Sources:

- The Hacker News
- FBI

Trojanized Claude Code Extension on Cursor Marketplace Plants SSH Backdoor

A tampered Claude Code extension, versions 2.1.312 and 2.1.313, was served on Cursor's marketplace on 29 October, reaching up to 5,000 users in 11 hours. The loader adds an attacker's SSH key, opens a reverse tunnel and sets up persistence, though Cursor says errors blocked SSH access on most macOS and Windows hosts. Anthropic says it did not build or publish the package.

Sources:

- OpenSourceMalware
- Microsoft Security Research

© CyberSecBrief 2025—2026

Threats

Attackers Abuse Microsoft Teams External Chat to Impersonate IT Support

More than 400 incidents involved attackers using Teams external chat, enabled by default, to pose as IT helpdesk staff, often after email bombing. Victims installed remote access tools such as Quick Assist, and payload execution followed in under 15 minutes.

Sources:

- Arctic Wolf

JFrog Finds 42 Hijacked GitHub Repositories Armed in testmetest npm Campaign

The 42 repositories belong to 11 legitimate owners and contain hooks for AI coding assistants and IDEs. Their payload wrappers decode to a hidden CI publisher that uses stolen tokens to publish malicious npm releases.

Sources:

- JFrog Security Research

Cyberattack Disrupts University of New Mexico Health Sciences Center

The centre detected a cybersecurity threat on 26 October that affected some end-user devices but not core systems. Ambulances were diverted for two hours, surgeries were suspended, and the BYOD ransomware group has reportedly claimed the attack.

Sources:

- University of New Mexico Health Sciences Center

Infrastructure & Exploits

Three Chained Flaws Behind Oracle PeopleSoft Zero-Day Enable Remote Code Execution

Oracle patched CVE-2026-35273 under one identifier although researchers reported three vulnerabilities. A server-side request forgery in the Integration Gateway reaches the Environment Management Hub, leading to remote code execution exploited by ShinyHunters.

Sources:

- Zero Day Initiative

Alpine Linux Rebuilds GitLab After Attempted CVE-2026-97229 Exploitation

An attacker crashed GitLab worker processes eight times on 20 and 21 October, and Alpine found no evidence of success but could not rule it out. GitLab's fix is a Ruby patch applied only in its own packages, which Alpine's image did not include.

Sources:

- Alpine Linux

16-Year-Old EDK2 Flaw Enables Pre-Boot Code Execution on Servers

CVE-2026-97631 is a buffer overflow in the PXE Base Code driver of TianoCore EDK II. An attacker on the local network can send an oversized ICMP error message during network boot to execute code before Secure Boot loads.

Sources:

- Ars Technica

Tools & Techniques

KeyDrift Malware Steals Encryption Keys From Cisco SD-WAN Controllers

UAT-11473 exploited CVE-2026-20127 to deploy KeyDrift, whose components extract keying material from decrypted control traffic inside vdaemon processes. Talos assesses with high confidence that the infrastructure overlaps with Volt Typhoon's Silent Train network.

Sources:

- Cisco Talos

VOLTA Infostealer Sends Stolen Data to an LLM to Rank Victims

The self-deleting Windows infostealer sends stolen credentials, sessions and wallet data to a language model through OpenRouter, which returns a ranking of the victim's assets. If the first model refuses, it falls back through two further models.

Sources:

- Cisco Talos

NetamLoader Malware Targets Custom Windows Build Used by Asian Governments

An unattributed actor delivered NetamLoader through a CAB archive in the Windows update folder, chaining XAML payloads that bypass AMSI and run inside dllhost.exe. Kaspersky identified one victim in Asia.

Sources:

- Kaspersky

Policy & Legal

Ukrainian Hacker Sentenced to 70 Months Over Nefilim and Hive Ransomware Attacks

Artem Stryzhak received 70 months as an affiliate of the Nefilim and Hive groups. Hive attacked about 1,500 victims between June 2021 and January 2023, causing more than $100 million in losses.

Sources:

- U.S. Department of Justice

Authorities Seize Domain of Bulletproof Hosting Provider Virtualine

US authorities seized virtualine.net, a bulletproof hosting provider advertised on cybercrime forums. Court records say it knowingly hosted a forum selling sexually explicit images of minors and accepted unhosted bitcoin payments.

Sources:

- U.S. Department of Justice

Syrian Electronic Army Hacker Jailed for 42 Months Over Attacks on Western Targets

Ahmad Umar Agha, known as “Th3Pr0”, was sentenced in a Virginia federal court for hacking about 47 Western media outlets, non-profits and allied entities. He was first charged in 2014 and taken into US custody last year.

Sources:

- The Record

Weekly Topic Distribution



Copyright and Legal Notice

© CyberSecBrief. All rights reserved.

Reproduction, redistribution, or modification of this document or its contents without explicit written permission is strictly prohibited.

Disclaimer & Terms of Use

CyberSecBrief is a personal, non-commercial project operated from Germany and is not affiliated with any company or organisation. The information provided is intended solely for general informational and educational purposes and does not constitute professional cybersecurity, legal, or financial advice. Security-related information changes rapidly; although accuracy and timeliness are sought, no guarantee is given regarding completeness, correctness, or applicability. Users must verify details with official sources or qualified professionals before making decisions.

The owner disclaims liability for any indirect, incidental, or consequential damages arising from reliance on this material. External links and third-party feeds are offered for convenience; their content, accuracy, availability, and privacy practices are outside our control and are not endorsed. Sponsored or promoted material may appear, yet inclusion does not imply endorsement.

Original content is protected by copyright. Where external material is used, appropriate attribution is provided. Reproduction of original content without prior written consent is prohibited. Content may be updated, modified, or removed at any time without notice.

This disclaimer and the Terms of Use are governed by the laws of Germany and applicable European Union regulations. Should any provision be deemed invalid, the remaining provisions shall continue in full force and effect.

Credits and Sources

CVE entries are sourced from the CVE® Program, operated by The MITRE Corporation, and from the National Vulnerability Database (NVD), maintained by the National Institute of Standards and Technology (NIST). The NVD is provided “as is” without warranty of any kind.

Definitions for APT groups are derived from the MITRE ATT&CK® knowledge base, reproduced and distributed with the permission of The MITRE Corporation. © 2025 The MITRE Corporation.

All feeds and advisories are properly acknowledged and linked to their original sources where referenced, including within briefings.

Logo icon created by Ida Desi Mariana — Flaticon.

Powered by CyberFeedBites.

Source

This briefing is published by *CyberSecBrief* –
https://www.cybersecbrief.com/