ISSUE / OCT 26 2026

MAG212 CYBER

CYBERSECURITY / INTELLIGENCE / TECHNOLOGY / PEOPLE

SHELL WEEK

REAL THREATS.
DEEP INSIGHTS.
PATCH FIRST.

PHP2Shell, Node2Shell and the race between the leak and the patch

- >_ **PHP2Shell**
  Exploited before the patch shipped
- { } **Node2Shell**
  One Brotli bug, many runtimes
- $ **SafePay**
  600+ ransomware victims
- AI **The Downloads trap**
  AI coding agents hijacked
- K **Kali 2026.3 & Japan**
  New tools, breach payouts



INSIGHTS TODAY. A SAFER TOMORROW.

THE EDITORIAL DESK

When the Leak Beats the Patch

This week the gap between "a fix exists" and "attackers have it" shrank to almost nothing. PHP2Shell was probed four days before its patch. Node2Shell turned one compression library into a problem for whole runtimes. Inside, we separate what was confirmed from what was claimed and give your team a patch-first plan.

9.2
CVSS 4.0 for each PHP2Shell flaw

59%
of 40,849 checked sites on a pre-fix PHP version

600+
SafePay victims since August 2024

INSIDE THIS ISSUE

03	PHP2SHELL	Two engine flaws, a leak and a four-day head start
04	DEFENDING THE RUNTIME	Where the flaw sits, patch matrix, verification
05	NODE2SHELL	How one Brotli bug spread across ecosystems
06	SAFEPAY RANSOMWARE	Joint advisory AA26-293A and the five CVEs to patch
07	THE DOWNLOADS TRAP	Planted instruction files vs. AI coding agents
08	BRIEFS & SOURCES	Kali Linux 2026.3, Japan's breach payouts

COVER STORY · EXPLOITED IN THE WILD

PHP2Shell: Four Days Ahead of the Patch

Two critical flaws in the PHP engine itself let an unauthenticated request run code on a web server. Exploitation began before most defenders knew the bugs existed.



CVE-2026-109618

Out-of-memory corruption

When a request hits PHP's memory limit, the engine can abort while internal request data is only half set up. Cleanup may then treat that broken data as valid.

CVE-2026-109619

Stale global state

Request-owned state can outlive the memory behind it, so a later request on the same worker may use it before the engine resets it.

Both flaws score 9.2 under CVSS 4.0 and affect every release before 8.5.12, 8.4.27, 8.3.36 and 8.2.35. Researchers at Wiz, Calif and OpenAI found them with AI-assisted research in August. The coordinated disclosure was moved up a day to October 21 after the CVE IDs leaked. Cloudflare reported millions of exploitation attempts after disclosure. As of October 23, neither CVE was in CISA's Known Exploited Vulnerabilities catalog.

INCIDENT CHRONOLOGY

17 OCT
First attempt in Amazon honeypot data

20 OCT
CVE IDs leak; CERT-EU warns

21 OCT
Patches ship; watchTowr sees exploitation

24 OCT
35 shells on 3 honeypots (Adel Karimi, Perplexity)

Why it matters: **honeypot attempts are not breaches.** Exposure, attempted exploitation and confirmed compromise are three separate facts, so record them separately in your incident ticket.

ARCHITECTURE & DEFENSE

Where the Flaw Lives

The bug sits below your application code. **Stopgap ≠ fix:** turning off `session.upload_progress` closes only one path for CVE-2026-109619 and does nothing for CVE-2026-109618.

01 INTERNET EDGE
Benign and hostile HTTP traffic

02 REVERSE PROXY / WAF
Rate-limit and block known abuse patterns

03 WEB SERVER
Apache mod_php or Nginx + PHP-FPM

04 PHP ENGINE
Memory-safety fault: the PHP2Shell layer

05 YOUR APP / CMS
Updating plugins here does not fix layer 04



PATCH MATRIX

8.5 branch	`8.5.12`
8.4 branch	`8.4.27`
8.3 branch	`8.3.36`
8.2 branch	`8.2.35`
8.1 and older	**End of life**

PATCH-FIRST CHECKLIST

0–2 H	**Scope:** list every internet-facing PHP service and its version, internet-facing ones first.
2–6 H	**Patch:** apply vendor or distro packages; check the distro tracker, not the version string.
6–12 H	**Verify:** restart FPM pools and Apache, then confirm the running binary is the patched one.
12–24 H	**Hunt:** look for PHP workers launching shells or download tools; rotate secrets if found.

RUNTIME SECURITY · CVE-2026-111497

Node2Shell: One Library, Many Blast Radii

An out-of-bounds write in Google's Brotli decoder, versions 1.0.3 through 1.2.0. A crafted compressed stream can corrupt memory in any program that decompresses untrusted Brotli data, causing a crash, a memory leak or possibly code execution.



`brotli 1.0.3–1.2.0 →` Node.js / Bun · Python · Java (Brotli4j) · .NET · Ruby · FFmpeg (JPEG XL) · ClickHouse · Apache Arrow

Node.js patched it first on October 21, so "Node2Shell" stuck. JFrog Security Research then showed the same flaw reachable through ClickHouse, FFmpeg, the .NET runtime and Apache Arrow, so the name undersells the reach.

Red Hat rates it Important (CVSS 3.1 score 8.1). No in-the-wild exploitation had been reported as of October 22.

Can't patch today? Reject requests carrying `Content-Encoding: br` at the proxy. Browsers don't compress request bodies, so real users won't notice.

UPDATE TO

Brotli	`1.0.10 / 1.1.1 / 1.2.1`
Node.js	`22.23.4 / 24.22.1 / 26.12.1`
Python	`Brotli ≥ 1.2.1`
Brotli4j	`1.24.0`
Ruby gem	`0.9.1`

Hidden risk: many packages **vendor their own copy** of Brotli. Updating the system library isn't enough, so scan container images and lockfiles too.

RANSOMWARE · ADVISORY AA26-293A

SafePay: 600 Victims and Counting

On October 20, the FBI, CISA, the US Secret Service and German and UK law enforcement warned that SafePay has hit at least 600 organisations across four continents since August 2024. Many of them are critical infrastructure.



HOW AN INTRUSION UNFOLDS

STOLEN / WEAK CREDENTIALS → UNPATCHED VPN & BACKUP → REMOTE TOOLS PERSIST → DATA STOLEN → BACKUPS HIT, FILES LOCKED

THE FIVE CVEs TO PATCH NOW

CVE-2020-3259	Cisco ASA / FTD
CVE-2023-20269	Cisco ASA / FTD VPN
CVE-2023-27532	Veeam Backup
CVE-2024-40711	Veeam Backup
CVE-2024-40766	SonicWall SonicOS

DEFENDER PRIORITIES

- Phishing-resistant MFA on every VPN and remote-access path
- Immutable, offline backups, tested for restore
- Segment the network; restrict admin rights
- Alert on unapproved remote-management tools
- Watch for large outbound transfers before encryption

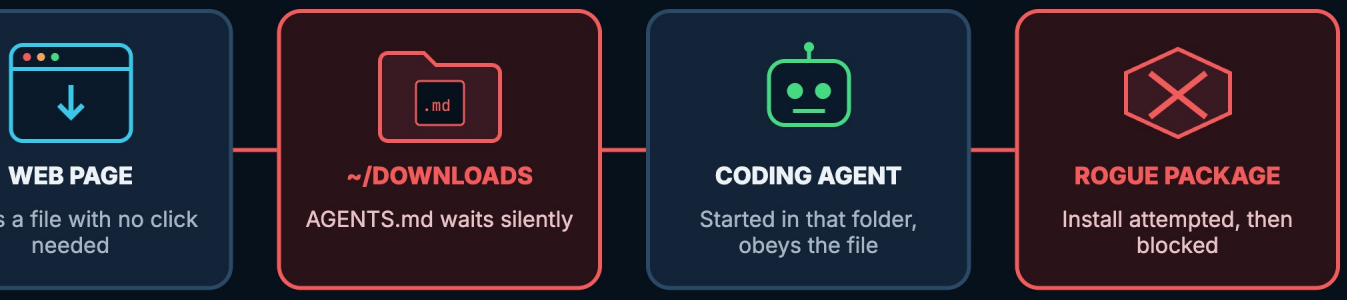
The pattern: SafePay mostly **logs in rather than breaks in.** Old VPN and backup flaws plus reused passwords do most of the work, so basic hygiene is the strongest control.

AI SECURITY · TRUST BOUNDARIES

The Downloads Trap

Forever Security found a planted `AGENTS.md` file in a customer's Downloads folder. That folder was also where their AI coding agent was running, and the agent tried to install a rogue npm package. The install was blocked before it ran.





The researchers' point: `~/Downloads` is the one folder a website can write to on its own, and coding agents are built to follow the instruction files they find where they run. Their tests affected both OpenAI's Codex and Anthropic's Claude Code.

GOVERNED AGENT HYGIENE

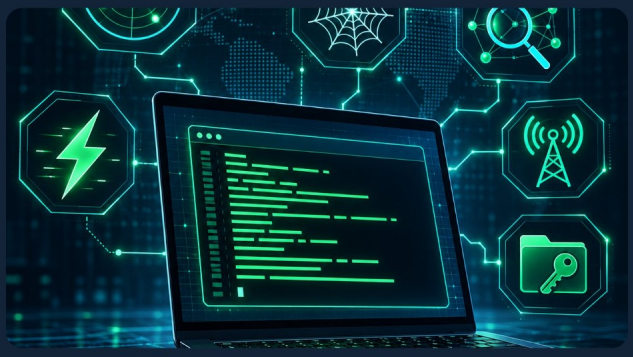
01 / SCOPE
Start agents from the project root, never from Downloads or your home folder.

02 / READ
Open any AGENTS.md or CLAUDE.md you didn't write before an agent sees it, including in fresh clones.

03 / REVIEW
Give instruction files owners and code review, just like source code.

04 / GATE
Keep approvals and sandboxes on, and don't use flags that bypass them.

BRIEFS



Kali Linux 2026.3

The third Kali release of 2026 updates 126 packages, moves the kernel from 6.19 to 7.1.5, ships KDE Plasma 6.7 and refreshes the image-build scripts.

`dalfox`	XSS scanner
`katana`	Web crawler
`qsreplace`	Query-string rewriter
`rustscan`	Fast port scanner
`sdrangel`	SDR front-end
`snaffler-ng`	SMB secrets finder



Japan Pays for Breaches

GMO Internet will compensate customers for losses from unauthorised access to its Onamae.com Desktop Cloud service and pay every current customer ¥5,000. It says it received an extortion demand and won't pay. Its shares fell almost 16%.

Park24 (Times car-sharing) is paying ¥3,000 per customer after a data breach. Japan has logged 723 incidents in 2026 so far, more than all of 2024 or 2025.

"The internet itself is now starting to break down."
— Masatoshi Kumagai, GMO CEO, to Reuters

PRIMARY SOURCES

PHP2Shell · SecurityWeek, Help Net Security, watchTowr, Tanium, AlmaLinux, Ubuntu

Node2Shell · JFrog Security Research, Red Hat RHSB-2026-015, Qualys, Aikido

AI agents · BleepingComputer, Help Net Security, CSO Online

Exposure data · Brandefense site checker, SOCRadar, The Hacker News

SafePay · CISA AA26-293A, GBHackers, HSToday

Briefs · BleepingComputer, Linuxiac, Reuters, Euronews

MAG212 CYBER

INSIGHTS TODAY. A SAFER TOMORROW.