

The one cyber threat that matters this week, and what to do about it — in plain English for business leaders.

Provided by Major Business Solutions LLC

HEADLINE THREAT

ACTIVE EXPLOITATION · CISA KEV

“PHP2Shell”: attackers are taking over websites through two critical flaws in PHP

On Monday, Oct. 26, CISA added **CVE-2026-109618** and **CVE-2026-109619** (both CVSS 9.2) to its Known Exploited Vulnerabilities catalog. Both let an attacker run code on a web server **without logging in**. PHP is the language behind most business websites, WordPress sites, customer portals and many vendor web apps; Censys estimates more than **32.5 million** PHP services are running an affected version. Amazon says exploitation attempts began Oct. 17, four days *before* fixes shipped, and a researcher confirmed a working takeover on Oct. 24. Fixed versions came out Oct. 21: **PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35** (Windows builds updated Oct. 26). CISA gave federal agencies until Oct. 29 to patch.

Why it matters for you

You probably don't run PHP yourself — but your website host, web developer, e-commerce platform or a vendor's customer portal almost certainly does. A hijacked site can serve malware to your customers, leak form data, or give attackers a foothold. The fix is a version upgrade, but **someone has to actually apply it**, and you may need to ask.

PATCH PRIORITY

KEV · OCT 26 **PHP — CVE-2026-109618 / CVE-2026-109619 (“PHP2Shell”).** Unauthenticated remote code execution. Upgrade to 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35 or later. Related: Brotli decoder flaw CVE-2026-111497 (fixed in 1.0.10 / 1.1.1 / 1.2.1).

KEV · OCT 23 **Nextcloud + Collabora Online built-in CODE server — CVE-2026-110447 (CVSS 9.2).** Command injection used to plant web shells and hunt for passwords and crypto wallets. Fixed in 26.4.303.

KEV · OCT 23 **Arista VeloCloud Orchestrator (on-prem SD-WAN) — CVE-2026-114625 (CVSS 9.9).** SQL injection, actively exploited; third exploited VeloCloud flaw since July. Fixed in 5.2.3.18 / 6.1.3.10 / 6.4.2.12.

CISA ALERT · OCT 16 **BeyondTrust Remote Support — CVE-2026-102764.** Auth bypass exploited as a zero-day since August; common MSP/IT support tool. Patch self-hosted 26.2.3-and-earlier appliances, and treat any that were internet-exposed as possibly compromised until reviewed.

KEV · OCT 20 **Plex Media Server — “Plex2Shell” (CVE-2026-96652/-96654/-96655/-96656).** Chained for takeover; used to drop crypto-miners. Update to 1.43.3.10861+ — or remove Plex from business networks.

BY THE NUMBERS

32.5M

PHP services running a version affected by PHP2Shell

Censys, via The Hacker News, Oct 2026

48%

of breaches involved a third party or supply chain, up from 30%

Verizon 2026 DBIR (Jun 2026)

~600

SafePay ransomware victims, mostly via stolen logins or unpatched edge devices

CISA/FBI #StopRansomware, Oct 22, 2026

\$4.99M

global average cost of a data breach — a record high

IBM Cost of a Data Breach 2026 (Jul 2026)

THREE ACTIONS THIS WEEK

1. **Ask your web host and website developer, in writing, to confirm PHP is patched — by Friday.** You want to hear “PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35 or later.” If a site runs an older, unsupported PHP, upgrade it or take it offline. Send the same question to any vendor that hosts a portal or app with your data.
2. **Check your remote-access and file-sharing tools.** Ask your IT provider/MSP whether you use BeyondTrust Remote Support, Nextcloud with Collabora, or VeloCloud SD-WAN. If yes, confirm they are patched and, for BeyondTrust, that the appliance was reviewed for signs of compromise.
3. **Harden Microsoft 365 against stolen-session attacks.** A BEC campaign tracked by Huntress replayed stolen login tokens to bypass MFA, then added its own MFA phone and hidden inbox rules. Turn on Conditional Access, review each user's MFA methods and inbox rules, and confirm your offline backups restore — SafePay ransomware's main entry points are stolen logins and unpatched edge devices.

How MajorCompliance can help

- For PHP2Shell and this week's other KEV additions, MajorCompliance checks each vendor's software bill of materials (SBOM) against the OSV.dev and NVD databases, and its Vulnerabilities page shows across all vendors which affected CVEs are on CISA's KEV list.
- To ask hosting and software vendors to confirm they've patched, MajorCompliance drafts the outreach email and gives each vendor a secure portal to respond, with a risk score and review schedule per vendor.
- If a vendor says PHP2Shell doesn't affect them, they can submit a VEX "not affected" statement with evidence, which is reviewed by AI and only counts once your own staff confirm it.

MajorCompliance is a vendor-risk platform from Major Business Solutions LLC.



Provided by Major Business Solutions LLC

SOURCES

1. [The Hacker News — CISA Confirms Active Exploitation of Two PHP2Shell Flaws Enabling Remote Code Execution \(Oct 27, 2026\)](#)
2. [BleepingComputer — Amazon says PHP2Shell exploitation began 4 days before patches \(Oct 22, 2026\)](#)
3. [CISA — CISA Adds Two Known Exploited Vulnerabilities to Catalog \(Oct 26, 2026\)](#)
4. [The Hacker News — CISA Flags Two Actively Exploited Critical Flaws in Collabora Online and Arista VeloCloud \(Oct 24, 2026\)](#)
5. [The Hacker News — CISA Orders Federal Agencies to Patch Exploited Plex2Shell, Siemens, and SiteGuard Flaws \(Oct 21, 2026\)](#)
6. [CISA — CISA Urges Patching Critical Vulnerability in BeyondTrust Remote Support \(Oct 16, 2026\)](#)
7. [BleepingComputer — BeyondTrust patches zero-day exploited in attacks since August \(Oct 16, 2026\)](#)
8. [CISA — #StopRansomware: SafePay Ransomware, AA26-293A \(Oct 22, 2026\)](#)
9. [Infosecurity Magazine — Widespread Token-Spraying Attacks Target Microsoft 365 Accounts \(Oct 23, 2026\)](#)
10. [Cyber Readiness Institute — 2026 Verizon Cyber Report: Small Businesses Face Escalating Cyber Threats \(Jun 1, 2026\)](#)
11. [eSecurity Planet — IBM 2026 Cost of a Data Breach Report: Key Findings \(Jul 30, 2026\)](#)
12. [CISA — Known Exploited Vulnerabilities Catalog](#)

Always verify advisories and patch versions directly with CISA (cisa.gov) and your vendors before acting. This briefing summarizes public reporting as of Oct 27, 2026, 11:00 UTC.