



One page. The threat that matters most right now, and what to do about it this week.

Provided by Major Business Solutions LLC

HEADLINE THREAT

ACTIVE — CISA ALERT

"PHP2Shell": two critical PHP flaws let attackers take over web servers — patch now

On Oct. 21, PHP shipped emergency fixes for **CVE-2026-109618** and **CVE-2026-109619** (both CVSS 9.2). Both are pre-authentication remote code execution bugs in the PHP engine itself, so even well-written sites are exposed. CISA told all organizations running PHP websites to patch right away. Amazon says the first attack attempts came on Oct. 17, four days before the patches. Cloudflare counted millions of attempts by Oct. 22, some trying to plant a Mirai-variant botnet. Researchers say most activity so far is scanning or broken exploits, but they expect working exploits soon.

Fixed versions: PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35. PHP 8.1 and older get no fix; move to a supported version or use your Linux distribution's backported patch.

Why it matters for you

PHP runs most WordPress, Drupal and Joomla sites, plus many customer portals, booking pages and online stores. Your website may run on a host, agency or vendor server you never think about. Censys found about 1.57 million internet-facing PHP hosts still unpatched as of Oct. 21, and VulnCheck counts at least 1 million on end-of-life versions. A hijacked web server can leak customer data, serve malware to your visitors, or become a foothold into your network.

PATCH PRIORITY

CRITICAL **WEBSITES** **PHP — CVE-2026-109618 / CVE-2026-109619 (PHP2Shell).** Update to 8.5.12 / 8.4.27 / 8.3.36 / 8.2.35. Under attack since Oct. 17. CISA alert issued Oct. 21.

EXPLOITED **REMOTE SUPPORT** **BeyondTrust Remote Support — CVE-2026-102764.** Authentication-bypass zero-day exploited since late August by a suspected China-linked espionage group. Cloud customers were patched Oct. 8. Self-hosted versions 26.2.3 and earlier must apply advisory BT26-05. Ask your MSP or IT provider if they use it.

CISA KEV

MEDIA SERVER

Plex Media Server — CVE-2026-96652, -96654, -96655, -96656 ("Plex2Shell"). Added to KEV on Oct. 20. The flaws chain into unauthenticated takeover and are being used to install crypto-miners and proxy malware. Fixed in 1.43.3.10861. Also added Oct. 20: SiteGuard Server Edition (CVE-2026-106931) and Siemens Software Center (CVE-2026-110936).

BY THE NUMBERS

4 days

Attacks on PHP2Shell began this long before patches existed

Amazon via BleepingComputer, Oct. 2026

~1.57M

Internet-facing PHP hosts still unpatched on Oct. 21

Censys via SecurityWeek, Oct. 2026

48%

Breaches involving a third party or supply chain, up from 30%

Verizon 2026 DBIR (via Cyber Readiness Institute)

96%

Ransomware victims that were small organizations

Verizon 2026 DBIR (via Cyber Readiness Institute)

THREE ACTIONS THIS WEEK

1. **Confirm your website's PHP version today.** Ask your web host, agency or IT provider in writing: "Are we on PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or a patched distro build?" If the site runs PHP 8.1 or older, schedule an upgrade. Until then, put it behind a web application firewall or take it offline.
2. **Ask about remote-access tools.** Have your MSP confirm whether it uses BeyondTrust Remote Support (self-hosted) and that the BT26-05 patch is in place. If the system was reachable from the internet before the patch, it should be checked for compromise.
3. **Inventory internet-facing software.** List every server, appliance and app your business exposes online, including side systems like a Plex media server. Patch anything on CISA's KEV list first, and turn off what you don't need.

How MajorCompliance can help

- For PHP2Shell, MajorCompliance checks each vendor's software bill of materials (SBOM) against the OSV.dev and NVD vulnerability databases and rescans on demand, so you can see which suppliers ship an affected PHP version.
- For BeyondTrust Remote Support and other vendor patches, MajorCompliance drafts the outreach email asking a vendor or MSP to confirm patching and gives them a secure portal to respond.
- If a vendor says it is not affected, it can submit a VEX "not affected" statement with evidence. The statement is reviewed by AI and counts only after your staff confirm it, and the finding stays visible either way.

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

Sources

1. [CISA — Critical Vulnerabilities in PHP Require Immediate Patching \(Oct. 21, 2026\)](#)
2. [SecurityWeek — PHP2Shell Exploitation Started Days Before Patches \(Oct. 22, 2026\)](#)
3. [BleepingComputer — Amazon says PHP2Shell exploitation began 4 days before patches \(Oct. 22, 2026\)](#)
4. [The Hacker News — PHP2Shell Exploit Attempts Hit Millions \(Oct. 23, 2026\)](#)
5. [SC Media — CISA advises orgs to patch PHP2Shell bugs immediately \(Oct. 21, 2026\)](#)
6. [BleepingComputer — BeyondTrust patches zero-day exploited in attacks since August \(Oct. 16, 2026\)](#)
7. [CISA — CISA Adds Six Known Exploited Vulnerabilities to Catalog \(Oct. 20, 2026\)](#)
8. [The Hacker News — CISA Orders Federal Agencies to Patch Exploited Plex2Shell, Siemens, and SiteGuard Flaws \(Oct. 21, 2026\)](#)
9. [Cyber Readiness Institute — 2026 Verizon DBIR: Small Businesses Face Escalating Cyber Threats](#)
10. [CISA — Known Exploited Vulnerabilities Catalog](#)

Always verify advisories, affected versions and patch details directly with CISA (cisa.gov) and your vendors before acting. This briefing is a summary, not a substitute for official guidance.