RT ProExec

ISSUED OCTOBER 22, 2026

Cyber Risk Alert

Severity: Critical | Action Required Now

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

CLIENT SECURITY ADVISORY

CRITICAL PHP FLAW: IS YOUR WEBSITE PATCHED?

The bottom line: Two critical security flaws were found in PHP, software that powers an estimated 70% of websites. They let an attacker take control of an unpatched web server over the internet, **with no password or login required**. Fixes were released on October 21, 2026, and attack attempts are already being reported. **Ask whoever manages your website or IT today to confirm that PHP has been updated and restarted.**

The Situation: What Happened

- **PHP is widely used.** It is a free programming language behind many business websites, online stores, customer and vendor portals, and platforms such as WordPress, Drupal, and Joomla. Many businesses use it without knowing it, because it can be built into a website, hosting service, or vendor software.
- **Two critical flaws were disclosed** (CVE-2026-109618 and CVE-2026-109619, nicknamed "php2shell"), rated 9.2 to 9.8 out of 10 for severity. The PHP project released emergency fixes on October 21, 2026.
- **Government agencies are urging immediate action.** The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the NSA, the FBI, and the UK's National Cyber Security Centre all advise patching right away.
- **Attackers are moving quickly.** Sample attack code is circulating publicly. CISA had not observed exploitation when it published its alert, but several security firms now report active attack attempts, and Amazon reports an attempt dated October 17, four days before the flaws were made public.

The Concern: Why It Matters to Your Business

A single specially crafted request could let an attacker run commands on an unpatched server. A compromised website or web server can expose a business to:

Data & credential theft Customer data, passwords, and keys on the server can be stolen.	**Ransomware & malware** A hijacked server can be used to install malicious software.	**Payment-card theft** Checkout and payment pages can be tampered with.
Website tampering Defacement, hidden redirects, or planted backdoors.	**Phishing from your domain** Attackers can send scams that appear to come from you.	**Business interruption** Downtime while systems are investigated and rebuilt.

- **Updating your website application is not enough.** The flaw is in PHP itself, so even a well-built, up-to-date website is exposed if the underlying PHP is old. After updating, PHP services must also be **restarted** for the fix to take effect.
- **Exposure can be hidden.** Your hosting company, web agency, or vendors may be running PHP on your behalf, so you may not know whether you are affected without asking.
- **Stolen secrets may leave few traces.** One of the flaws can also expose data held in server memory, such as passwords and API keys, without leaving obvious signs of a break-in.

Go-Forward Guidance: What To Do

You do not need to diagnose this yourself. Ask your technology provider to handle it and confirm in writing.

TODAY

1. **Contact whoever runs your website:** your IT team, web developer, digital agency, managed service provider, or hosting company. Send them the question in the box below.
2. **Have PHP updated and restarted.** Every PHP installation should be on version **8.5.12, 8.4.27, 8.3.36, or 8.2.35** (or a patched version from your hosting or software vendor), with web services restarted afterward. Public-facing systems come first.
3. **If it can't be patched right away, take it offline** until it can. CISA, the NSA, the FBI, and the UK NCSC all advise this. A web application firewall may add some protection but is not a substitute for the update.

THIS WEEK

4. **Look beyond the main website.** Include secondary and test sites, customer and vendor portals, online payment pages, and any vendor software or hosted tools that may have PHP built in.
5. **Check for signs of compromise going back to October 17, 2026.** Ask your provider to review server logs and systems for suspicious activity, since attacks were reported before the fixes were public.
6. **Consider changing credentials** (admin logins, database passwords, API keys) stored on any server that ran unpatched PHP.
7. **Retire unsupported PHP.** PHP 8.1 and older no longer receive official fixes and are at higher risk. Move to a supported version or a vendor-patched build. PHP 8.2 reaches end of life on December 31, 2026, so plan ahead.
8. **Ask key vendors** that handle your data whether they use PHP and whether they have applied the fix.

KEEP PROOF

9. **Get written confirmation of** PHP versions, patch dates, service restarts, and log reviews, and keep it on file.

COPY AND SEND THIS TO YOUR WEBSITE OR IT PROVIDER

"Do any of our websites, portals, or internet-facing applications use PHP, directly or inside vendor software? If so, please confirm in writing: (1) the PHP version on each system; (2) that it is now 8.5.12, 8.4.27, 8.3.36, 8.2.35, or a vendor-patched version; (3) that PHP services were restarted after the update; and (4) that logs were reviewed for suspicious activity since October 17, 2026."

KNOWN OR SUSPECTED INCIDENT? REPORT IT TO YOUR CYBER INSURANCE CARRIER

- **Pause before you wipe or rebuild.** Preserve logs and affected systems so investigators can determine what happened.
- **Report any known incident to your cyber insurance carrier promptly, in accordance with the claims reporting requirements in your policy.** Cyber policies may contain specific notice requirements and may require the insurer's consent before certain response vendors are engaged or costs are incurred. Review the applicable policy and contact your broker or carrier promptly.
- **Watch for warning signs:** unfamiliar files on the server, defaced or redirected pages, unexpected crashes or errors, unusual outbound traffic, or customers reporting odd emails or links from your domain.
- **Document your patching.** Patching practices and use of unsupported software may be relevant to underwriting and claims considerations, depending on the circumstances and applicable policy terms. Keep your written confirmations and review your policy terms with your broker.

FOR YOUR IT OR WEB TEAM: TECHNICAL SUMMARY

- **Flaws:** CVE-2026-109618 (memory corruption during out-of-memory handling) and CVE-2026-109619 (stale request state; can also disclose memory). Both allow unauthenticated remote code execution. CVSS 9.2 (PHP, v4.0) and 9.8 (NVD, v3.1).
- **Affected:** all PHP installs serving web requests (mod_php, PHP-FPM, php-cgi, FrankenPHP, LiteSpeed), with mod_php rated highest risk. Any version before 8.5.12, 8.4.27, 8.3.36, or 8.2.35. PHP 8.1 and older are unsupported; use distribution/LTS backports, upgrade, or PHP's published source backports (7.4, 8.0, 8.1).
- **Fix:** upgrade or install the vendor's patched package, then restart Apache, PHP-FPM, and all long-running workers. Prioritize internet-facing systems and inventory embedded PHP (CMS, appliances, control panels, containers). NCSC-NL maintains a list of software that bundles PHP.
- **Interim measures** (for example, disabling session.upload_progress and limiting request sizes) only reduce exposure; patching is the only complete fix.
- **Hunt from October 17:** oversized or malformed PHPSESSID cookies; unusual multipart uploads followed by memory-limit errors or repeated HTTP 500s; PHP worker crashes or restarts; PHP workers spawning shells or downloading tools. A clean result does not prove a system is safe.

FOR AGENTS AND BROKERS: Please share this alert with your clients and encourage them to forward it to whoever manages their website or IT environment. Clients do not need to diagnose the issue themselves. What matters now is getting written confirmation from their technology provider that PHP has been updated and restarted.

SOURCES AND CITATIONS

This is a fast-moving situation, and details may change.

CISA alert "Critical Vulnerabilities in PHP Require Immediate Patching" (Oct. 21, 2026); PHP project security advisory (php.net); CERT-EU Security Advisory 2026-018; NCSC-NL php2shell repository; Amazon Threat Intelligence and watchTowr reporting.

RT ProExec is a part of the RT Specialty division of RSG Specialty, LLC, a Delaware limited liability company based in Illinois. RSG Specialty, LLC, is a subsidiary of Ryan Specialty, LLC. RT ProExec provides wholesale insurance brokerage and other services to agents and brokers. RT ProExec does not solicit insurance from the public. Some products may only be available in certain states, and some products may only be available from surplus lines insurers. In California: RSG Specialty Insurance Services, LLC (License #0G97516). ©2026 Ryan Specialty, LLC

This alert is provided for general risk-management purposes and is not a coverage determination or technical advice. Coverage is subject to the terms, conditions, limitations, and exclusions of the applicable policy. This alert is provided for general information purposes only and does not constitute legal, technology, cybersecurity or professional advice. No warranties, promises, and/or representations of any kind, express or implied, are given as to the accuracy, completeness, or timeliness of the information provided in this alert. No user should act on the basis of any material contained herein without obtaining proper legal or other professional advice specific to their situation. Information is current as of October 22, 2026.