

Service

Data Privacy &
Cybersecurity

Professionals

ERIK DULLEA
DENVER:
303.749.7270
ERIK.DULLEA@
HUSCHBLACKWELL.COM

BENJAMIN PERRY
NASHVILLE:
615.949.2254
BENJAMIN.PERRY@
HUSCHBLACKWELL.COM

Critical PHP Vulnerabilities Under Active Exploitation Attempts: Six Questions for Your IT Team Today

Key point: Two newly disclosed critical vulnerabilities in PHP could allow an unauthenticated attacker to remotely execute code on affected web servers. The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are urging organizations to identify systems using PHP and patch them immediately, prioritizing internet-facing systems.

Organizations should act quickly to address two critical PHP vulnerabilities disclosed on October 21, 2026. The vulnerabilities, CVE-2026-109618 and CVE-2026-109619, collectively referred to as “PHP2Shell,” affect PHP installations serving web requests and can permit unauthenticated remote code execution. Exploitation attempts were reported even before the patch was released.

PHP is an open source, server-side scripting language used to build dynamic websites and web applications. Instead of running in the visitor’s browser, PHP code runs on the web server, where it processes requests, talks to databases, and generates the HTML that users see. It powers many popular platforms, including WordPress, Drupal, and Laravel-based sites. PHP can also be embedded in third-party software, meaning its presence within an organization may not always be readily apparent.

Because PHP runs on the server itself, an unauthenticated remote code execution flaw can let an outsider run commands on that server without a password or login. In practice, an attacker could install malware or ransomware, steal customer, employee, or other sensitive data stored on or accessible from the server, alter or deface the website, create hidden “backdoor” access for later use, or use the compromised server as a stepping stone to other systems on the organization’s network. For general counsel and other business leaders, the immediate task is not to grasp the technical details

of PHP2Shell. It is to ask the right questions, identify obstacles to remediation, and give the people responsible the resources to act.

Six Questions to Ask Your IT Team Today

1. Do we have PHP in our environment, and do we know where it is?

The NSA recommends an immediate inventory of services reliant on vulnerable PHP versions. Ask IT whether that inventory exists and covers cases in which PHP is a component of other software or runs on systems managed by vendors or hosting providers. Assume the risk goes beyond your public-facing websites.

2. Have we identified and prioritized our internet-facing PHP systems?

CISA recommends prioritizing internet-facing systems for patching. Ask whether the organization's inventory identifies which PHP systems are externally accessible and whether those systems are receiving priority for remediation.

3. Have affected systems been patched?

The PHP Project has released patched versions 8.5.12, 8.4.27, 8.3.36, and 8.2.35 and states that updating is the only safe choice. Organizations should ask which affected PHP systems have been patched and when patching of the remaining systems will be completed.

If your organization is running older or unsupported versions of PHP (8.1 and earlier, which no longer receive regular updates), ask: Have we confirmed with our vendor whether a backported fix is available? If not, what is our plan to upgrade or retire those systems?

Organizations moving to 8.2.35 should also note that PHP 8.2 reaches end of life on December 31, 2026, after which it will receive no further security fixes.

4. If we cannot patch immediately, what are we doing with the affected systems?

When immediate patching is not feasible, ask what steps can be taken to reduce the organization's exposure. Interim measures can help, but the PHP Project is clear that they are not a substitute for patching.

Both the NSA and CISA recommend taking a system offline if it cannot be patched promptly. This is where business decisions may be necessary. Taking a system offline can affect operations or customers, but leaving a vulnerable system exposed carries its own risk.

5. Are we looking for signs that someone may already have exploited these vulnerabilities?

Patching fixes the vulnerabilities, but the NSA expects cyber actors to weaponize PHP2Shell, and some security researchers report that exploitation attempts have already begun. Ask whether potentially affected systems are being reviewed or monitored for suspicious activity.

If the organization identifies indications of potentially malicious activity, consider promptly involving legal counsel and the incident-response team so the organization can appropriately investigate, preserve relevant evidence, and evaluate potential contractual, regulatory, or notification obligations (including state breach-notification laws and, for public companies, SEC reporting).

6. What resources or decisions does IT need from the company today to materially reduce our risk?

This may be the most important question for business leaders to ask.

Responding to a critical vulnerability can require more than directing IT to “patch immediately.” The team may need additional personnel, outside technical support, expedited assistance from a vendor, authority to take a system offline, or management support to prioritize remediation over other business activities.

The goal is to identify whether resource constraints, operational needs, or delays in decision-making are preventing the IT and cybersecurity teams from materially reducing the organization’s exposure today.

What This Means for You

Business executives do not need to become PHP experts, but they should ask whether the organization knows where PHP is running, whether affected systems have been patched, and what IT needs from them to move faster. Use the six questions above as a checklist in conversations with IT and security leadership this week, and document the answers.

If IT cannot confirm that internet-facing PHP systems have been inventoried, prioritized, and patched, ask what is standing in the way and whether additional resources, vendor support, or authority to take systems offline would help. If there are signs that a system may already have been compromised, loop in legal counsel promptly so that privilege, evidence preservation, and notification obligations can be assessed alongside the technical response.

Critical vulnerabilities are not solely an IT issue. Cybersecurity has become a key element of business risk. When urgent remediation is required, senior management has an important role in removing the business obstacles that stand between identifying a new risk and controlling it.

This article provides general legal information. It does not constitute legal advice to the reader and does not create an attorney-client relationship between the reader and Husch Blackwell LLP. The reader should seek legal advice if they have questions about how this legal information may apply

to their own circumstances.