PHP2Shell Vulnerabilities: Teqnovos Offers Security Patch Deployment and PHP Upgrade Support

Teqnovos's assistance addresses production patching and compatibility decisions for organizations managing legacy PHP applications.

NEW YORK, NY, UNITED STATES, October 22, 2026 /EINPresswire.com/ -- Teqnovos announced PHP2Shell patch deployment and PHP upgrade support following PHP's October 21, 2026, security release. The vulnerabilities, CVE-2026-109618 and CVE-2026-109619, have a critical Common Vulnerability Scoring System (CVSS) version 4.0 score of 9.2 and can allow unauthenticated remote code execution. The service combines production patching with compatibility testing for legacy applications.

> "PHP2Shell is one of the most serious PHP threats in years. Our job is to help every business patch fast and verify it, without breaking the systems their customers rely on."
>
> *Ankur Magan*

What Is PHP2Shell?

The PHP2Shell vulnerabilities have Common Vulnerabilities and Exposures (CVE) identifiers CVE-2026-109618 and CVE-2026-109619. According to the PHP project's security advisory, they affect PHP installations serving web requests and can allow unauthenticated remote code execution. The project urges immediate updates and identifies updating as the only complete solution.

Teqnovos's PHP2Shell vulnerability fix guide covers runtime verification and temporary controls when patching is delayed. It also outlines steps for investigating suspected compromise separately from patch deployment.

How Teqnovos Helps Businesses Patch PHP2Shell

The engagement draws on Teqnovos's application maintenance services. It covers runtime discovery and assessment against vendor advisories. The work includes patch deployment alongside compatibility and regression testing. Remediation records document completed work and unresolved upgrade requirements.

What If You're Running PHP 8.1 or Older?

The official fixed releases are PHP 8.5.12, PHP 8.4.27, PHP 8.3.36, and PHP 8.2.35. PHP 8.1 and

older no longer receive regular PHP project security updates. Some vendors provide backported fixes.

The PHP project also published minimal source backports for PHP 7.4 and PHP 8.0 as well as PHP 8.1. These patches do not restore regular support for those branches. Application owners need to verify their specific build against the relevant vendor advisory before choosing between a patched package and a move to a supported branch.

Teqnovos's Web4Realty case study documents the modernization of a legacy Zend Framework application through Laravel refactoring and automated testing. It provides background on the company's experience with legacy application compatibility.

Verifying the Patch Is Live

Runtime verification checks the package or build serving live requests against the relevant vendor advisory. Where required, affected workers or services need to be restarted before the running build is checked again. Separate checks cover PHP bundled inside containers and third-party products.
Patch verification confirms deployment status. Establishing whether an attacker previously accessed a system requires a separate investigation.

Request a PHP runtime and patch-readiness assessment from Teqnovos. Identify affected environments and define patch deployment, verification, and legacy upgrade requirements.

About Teqnovos
Teqnovos develops artificial intelligence (AI) solutions and custom digital products for startups and enterprises. Its AI-driven software development services span mobile applications, web platforms, healthcare software, and financial technology. The company also develops software-as-a-service products and blockchain solutions and provides dedicated development teams.

Media Contact
Teqnovos
Email: info@teqnovos.com
Phone: +1 628-800-0607
Website: https://teqnovos.com/

William Herbert
Teqnovos
+1 628-800-0607
Visit us on social media:
LinkedIn
Instagram
Facebook

X

This press release can be viewed online at: https://www.einpresswire.com/article/951505304

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.