

Critical PHP Security Update: What Website Owners Should Know

Public vulnerability update issued October 21, 2026 | Example customer bulletin for Custom Post testing

What happened

On October 21, the PHP project released fixes for two critical vulnerabilities in the PHP runtime, **CVE-2026-109618** and **CVE-2026-109619**. These issues, sometimes collectively called **PHP2Shell**, can expose unpatched internet-facing PHP installations to attacks that may lead to remote code execution without prior authentication.

PHP runs behind the scenes on many websites, including WordPress installations. The issue is in PHP itself, not a newly discovered WordPress-specific flaw.

PHP security releases

8.2.35	8.3.36	8.4.27	8.5.12
Fixed PHP 8.2 release	Fixed PHP 8.3 release	Fixed PHP 8.4 release	Fixed PHP 8.5 release

Versions older than these releases in their respective branches require evaluation and patching. End-of-life installations require special attention; a vendor-supported backport may differ from the upstream version number.

Guru Internet Services response

Guru Internet Services reports that it has already performed the appropriate PHP security upgrades across the servers it manages for customers. The agency emphasizes proactive infrastructure maintenance and reducing avoidable exposure to newly disclosed vulnerabilities.

That update status is a company-provided statement for this test. The technical version details and any assertion about specific server configurations should be confirmed against operational records before public publication.

Why this matters to customers

Timely server maintenance helps reduce the period in which vulnerable software is exposed. Security is ongoing work, however: a successful update is an important control, not a guarantee that every possible risk has been eliminated. Customers with questions about their managed hosting can contact Guru Internet Services.

Official sources

[PHP Security Release and Advisory \(October 21, 2026\)](#)

[WordPress.org: Critical PHP Security Release](#)

For test use: This is an example source document created to evaluate a draft-writing workflow. It is not an independent audit, assurance certificate, or verified infrastructure report.