Trusted Partners
Founded 1985

TS PARTNERS

610.768.1100
info@tspartnersinc.com
tspartnersinc.com

October 21, 2026

PHP2Shell Vulnerability
CVE-2026-109618 and CVE-2026-109619
(CVSS Rating 9.2 of 10 – Critical)

What is "PHP"?

PHP: Hypertext Preprocessor ("PHP") is a widely used, open-source server-side scripting (programming) language designed primarily for web development. It allows developers to create dynamic website content, interact with databases, and handle backend application logic.

Unlike client-side languages like JavaScript (which run directly inside your web browser), PHP code runs entirely on the **web server**. The server processes the PHP script and sends the final result back to your browser as plain HTML, meaning the user never sees the actual PHP code.

PHP is estimated to power roughly **75% to 80%** of all websites that use a known server-side language, since it serves as backbone for popular content management publishing systems (CMS) like **WordPress** and Drupal, and ecommerce platforms like Adobe's Magento.

PHP2Shell refers to two critical, unauthenticated remote code execution (RCE) and memory leak vulnerabilities in the PHP core runtime, being tracked as **CVE-2026-109618** and **CVE-2026-109619**. These flaws carry a critical severity rating of **CVSS 9.2**.

Critical Vulnerabilities

The PHP Foundation revealed twp serious vulnerabilities. PHP developers have released emergency security updates to fix critical flaws that could be exploited and allow bad actors to gain remote control of targeted systems. Security experts warn of potential dire consequences of overlooking unpatched systems.

PHP Foundation wrote in its advisories:

all PHP installations serving web requests going back to PHP version 5, released in July 2004. However, only PHP 8.2 and newer are still supported and will receive patches, according to the alert. (The PHP Foundation noted, though, that some PHP distributions and third-party vendors still produce legacy fixes.)

"There are no complete mitigations, updating is the only safe choice,"

TS Partners – Statement:

"PHP is not used by TSP for any publicly-exposed services or shipped software products. PHP is not required by or recommended for any of TSP's deployed applications."

Additional Information:
https://nvd.nist.gov/vuln/detail/cve-2026-109618
https://nvd.nist.gov/vuln/detail/cve-2026-109619

Headquarters
630 Freedom Business Center Dr., Ste. 212 King of Prussia, PA 19406 USA
Offices
1411 K St. NW Washington, DC 20005 USA