THREAT ADVISORY · CRITICAL · UNAUTHENTICATED RCE

PHP2Shell

CVE-2026-109618 | CVE-2026-109619

On 10/21/26, PHP disclosed two critical vulnerabilities, CVE-2026-109618 and CVE-2026-109619 ("PHP2Shell"), that allow for unauthenticated remote code execution. VulnCheck researchers independently reproduced both vulnerabilities the night the news leaked.

01 / WHAT WE'RE SEEING

VulnCheck exploit achieves RCE on ASLR-enabled systems

The VulnCheck Initial Access Intelligence Team has a working RCE exploit for CVE-2026-109618 on x86-64 with ASLR enabled on several PHP 8.4.x versions, along with more than a dozen network rules. We don't know of any other public or commercial exploits that are able to exploit multiple PHP versions under realistic production configurations.

Massive exposure

VulnCheck Target Intelligence found PHP on 2.6M+ internet-facing hosts, and 99.998% of them are vulnerable or likely vulnerable.

2.6M+
HOSTS RUNNING PHP

99.998%
VULNERABLE OR LIKELY

No fix for many

About 1.1M hosts (42%) run end-of-life PHP branches with no official patched release. (PHP has released guidance and updates on their site @ the PHO New Archive)

Hidden PHP

469K+ WordPress and 124K+ Laravel hosts run on PHP. Even if a system doesn't advertise PHP, it can still be exposed.

Active in the wild

VulnCheck Canaries have recorded growing numbers of attempted PHP2Shell exploitation. We observed attackers adopting at least five public exploit kits within a day, including one multi-stage attempt to bypass ASLR.

A flood of bad PoCs

Our research team has reviewed hundreds of public proof-of-concept repositories, most of which are fake or otherwise demonstrate artificial lab scenarios. VulnCheck Exploit and Vulnerability Intelligence data is being updated continuously as our team reviews new PoC code.

02 / WHAT TO DO

A
Patch to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35.

B
Can't patch yet? Apply the interim mitigations in the PHP advisory.

C
Hunt and block using the IOCs in the VulnCheck research: attacker IPs, user agents and web shell artifacts.