SPECIAL EDITION / 22 OCTOBER 2026

Special edition: CVE-2926-109618 (Update #2)

PHP fixes are out; exploitation attempts are reported, and FPM isn't exempt

4 stories / Listen online - 3:27

THE TAKEAWAY

PHP's leaked core flaws have moved from embargo drama to a patching job. Fixes are available, and FPM isn't a blanket exemption. This assessment is current to 09:40 NZDT on 22 October, or 07:40 AEDT.

01 / THE BRIEF

What changed

Since our previous assessment, PHP has published fixes, technical advisories and both CVE records. watchTowr now reports active exploitation attempts against both vulnerabilities. That's an attributed observation, not independently verified successful compromises or a measured global campaign. Some legacy installations also have backport routes.

SOURCES

PHP - Security advisory: Critical remote code execution vulnerabilities, update now - Primary source

CVE-2026-109618 - PHP CNA record - Primary source

CVE-2026-109619 - PHP CNA record - Primary source

PHP2Shell: PHP Remote Code Execution Exploited - Primary source

php2shell: Patched PHP packages available in testing - Primary source

02 / THE BRIEF

An older discovery, an early leak

CVE-2926-109618 appears to be a typo in a quoted watchTowr post; PHP's published identifier is CVE-2026-109618.

Wiz says it reported the vulnerabilities on 24 August. Their existence leaked on Hacker News on 20 October; PHP subsequently scheduled fixes for 21 October at 14:00 UTC. That was the announced schedule, not an established actual release minute.

SOURCES

PHP RCE Zero-Days CVE-2026-109618, CVE-2026-109619 Leak Early - Reporting / context

Tell HN: 2x PHP RCE CVEs with CVSS 10.0 Incoming - Primary source

Upcoming Critical PHP Security Release - Primary source

PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet - Primary source

CVE-2026-109618 - PHP CNA record - Primary source

03 / THE BRIEF

FPM isn’t off the hook

Both bugs carry official CVSS v4.0 scores of 9.2. CVE-2026-109618 leaves partially initialised memory reachable after an out-of-memory abort. CVE-2026-109619 leaves freed request state available for a later request in the same worker to consume. Neither is an application-framework bug.

PHP places all installations serving web requests in the at-risk population. mod_php has the highest demonstrated risk, including exploitation before application code runs. For CVE-2026-109618, PHP confirms complete HTTP RCE against mod_php, but says a complete FPM exploit hasn’t been demonstrated.

The second flaw has confirmed RCE paths against both mod_php and FPM. The validated FPM path requires a suitable application operation after request startup, so configuration and application behaviour matter. “Every PHP site falls instantly” overstates the evidence; “we use FPM” doesn’t settle it either.

Successful exploitation runs code with the web worker’s privileges, not automatically as root. PHP also confirms memory disclosure for the stale-state flaw.

SOURCES

RCE via OOM corruption - Primary source

RCE via stale global state - Primary source

PHP - Critical remote code execution security advisory - Primary source

PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet - Primary source

Rapid Response: php2shell, Leaked Critical PHP Vulnerabilities - Primary source

04 / THE BRIEF

Check the package and the running worker

Upstream fixes are 8.5.12, 8.4.27, 8.3.36 and 8.2.35. Distribution backports can look older: Ubuntu 24.04's 8.3.6-0ubuntu0.24.04.13 fixes both. Check the full package build, not just the upstream-looking version.

PHP has supplied minimal source backports for 7.4, 8.0 and 8.1 without restoring normal support. AlmaLinux's 17:50 UTC update on 21 October puts its 7.4 fix in production and its other shipped streams in testing.

WORTH ASKING

If you're on Laravel Forge, automatic security updates don't cover PHP. Update each installed version, verify the repository offers a fixed build and restart long-running PHP processes. PHP says updating is the only complete solution; configuration switches block particular paths, not the whole problem.

SOURCES

PHP - Security advisory and update instructions - Primary source

CVE-2026-109618 | Ubuntu - Primary source

CVE-2026-109619 | Ubuntu - Primary source

php2shell: Patched PHP packages available in testing - Primary source

PHP security advisory (CVE-2026-109618, CVE-2026-109619) - Laravel Forge - Primary source

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.