SPECIAL EDITION / 23 OCTOBER 2026

Special edition: CVE-2926-109618 (Update #3)

A reported compromise and a pre-disclosure attempt broaden the investigation window

5 stories / Listen online - 3:49

THE TAKEAWAY

PHP2Shell has moved beyond reported attempts: Sophos now reports a successful compromise. Patches are available, but the investigation window starts before disclosure. Current to 06:25 NZDT on 23 October, or 04:25 AEDT.

01 / THE BRIEF

What changed

Since Update #2, the evidence has strengthened: Sophos reports successful exploitation, AWS identifies an earlier attempt, VulnCheck describes an ASLR-bypassing exploit, and AlmaLinux's remaining fixes have reached production.

Sophos's 22 October, 16:18 UTC update reports malware execution, apparently a Mirai variant called potassium. That remains Sophos's observation, not an independently inspectable victim investigation. It hadn't observed evidence connecting the activity to ransomware, data theft or supply-chain compromise.

AWS dates a MadPot exploitation attempt to 17 October, but doesn't establish whether it would have succeeded against a real system or how the actor obtained exploit information. Its recommendation is to investigate from at least that date, not disclosure.

VulnCheck says its commercial CVE-2026-109618 exploit achieved RCE on PHP 8.4.26, x86-64, with ASLR enabled and display_errors disabled. Its ARM64 RCE attempt failed. Those are specified test conditions, not universal exploitability.

SOURCES

Amazon Threat Intelligence identifies PHP2Shell exploitation prior to public disclosure in MadPot - Primary source

Proof-of-concept exploit released for PHP vulnerabilities (CVE-2026-109618, CVE-2026-109619) - Primary source

PHP2Shell Vulnerabilities: CVE-2026-109618 and CVE-2026-109619 - Primary source

php2shell: Patched PHP packages released - Primary source

02 / THE BRIEF

The leak wasn’t the beginning

The published identifier is CVE-2026-109618; CVE-2926-109618 appears to be a typo in a quoted watchTowr post. Its companion is CVE-2026-109619. Wiz says it reported the flaws on 24 August. Their existence leaked publicly on 20 October; PHP released fixes on 21 October.

SOURCES

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

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

03 / THE BRIEF

FPM still isn’t an exemption

These are PHP-core lifecycle bugs, both rated CVSS v4.0 9.2. CVE-2026-109618 leaves incompletely initialised memory reachable after an out-of-memory abort. CVE-2026-109619 leaves freed request state for a later request in the same worker to consume.

PHP puts all web-serving installations in scope. mod_php has the highest demonstrated risk, including RCE before application code runs. PHP hasn’t demonstrated a complete FPM exploit for the first flaw; the second has confirmed FPM RCE requiring suitable application behaviour after startup. FPM isn’t a get-out-of-patching card.

Impact includes code execution as the web worker and memory disclosure, not automatic root access.

SOURCES

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

RCE via OOM corruption - Primary source

RCE via stale global state - Primary source

04 / THE BRIEF

Check the build, then replace the workers

Upstream fixes are 8.5.12, 8.4.27, 8.3.36 and 8.2.35. Backports can look older: Ubuntu 24.04’s 8.3.6-0ubuntu0.24.04.13 fixes both. Minimal source backports exist for 7.4, 8.0 and 8.1 without restoring normal support.

AlmaLinux's production rollout began at 21:15 UTC on 21 October; use its production repositories and verify the full package build. Forge's automatic security updates exclude PHP: update every installed version and restart long-running processes. PHP says configuration workarounds aren't a complete solution.

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 released - Primary source

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

05 / THE BRIEF

Don't stop at websites

NZ NCSC also flags PHP embedded in firewalls, edge devices and other platforms: those may need separate vendor remediation. Patching doesn't remove an existing compromise. Victim numbers, campaign scale and NZ/AU impact remain unresolved.

SOURCES

UPDATED: CVE-2026-109618 and CVE-2026-109619 affecting PHP - Primary source

NCSC encourages immediate patching against PHP vulnerability - Primary source

Critical vulnerabilities in PHP - Primary source

Vulnerabilities in PHP Affecting Cisco Products: October 2026 - Primary source

PHP web runtimes (CVE-2026-109618 and CVE-2026-109619) - 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.