SPECIAL EDITION / 25 OCTOBER 2026

Special edition: CVE-2926-109618 (Update #5)

Exploit claims widen; NetScaler fixes are pending and a compromise account needs qualification

5 stories / Listen online - 3:33

THE TAKEAWAY

PHP2Shell now has broader claimed exploit coverage, with several appliance fixes still pending. The evidence doesn't establish widespread successful compromise. Current to 08:26 NZDT on 25 October, or 06:26 AEDT.

01 / THE BRIEF

What changed

Since Update #4, VulnCheck's 23 October, 21:30 UTC update expands its commercial mod_php exploit claim to PHP 8.5.10-8.5.11, AMD64 and ARM64, and supported default WordPress Docker deployments. Previously, it listed PHP 8.4.10-8.4.26. This is vendor testing, not independent validation across production builds.

New supplier findings and a qualified Unit 42 compromise account also extend the picture.

SOURCES

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

Threat Brief: Critical Vulnerabilities in PHP: CVE-2026-109618, CVE-2026-109619 (Updated October 23) - Primary source

Cloud Software Group Communication Regarding Recent PHP Vulnerabilities - Primary source

PHP web runtimes (CVE-2026-109618 and CVE-2026-109619) - Primary source

02 / THE BRIEF

The underlying risk

The documented flaws are CVE-2026-109618 and CVE-2026-109619. They leave incompletely initialised or freed request state for later code to consume. PHP puts all web-serving installations in scope.

mod_php has demonstrated RCE before application code runs. FPM has validated RCE for the second flaw, dependent on application behaviour; no complete FPM exploit is demonstrated for the first. Execution is as the web worker, not automatically root.

SOURCES

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

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

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

03 / THE BRIEF

Attempts aren't a victim count

AWS reports a MadPot attempt on 17 October, before the 20 October public leak, and recommends investigating from at least 17 October. Success against real systems remains unclear.

Sophos's 22 October, 21:21 UTC correction stands: failed attempts, not successful compromise in its telemetry.

Unit 42's 23 October revision reports access to password hashes and MFA secrets at an unnamed European government entity, plus attempted Domain Admin escalation. It doesn't establish the initial-access CVE or attack date. This isn't a confirmed PHP2Shell victim.

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

Honeypot Observations on PHP Vulnerabilities CVE-2026-109618 and CVE-2026-109619 (php2shell) - Primary source

Threat Brief: Critical Vulnerabilities in PHP: CVE-2026-109618, CVE-2026-109619 (Updated October 23) - Primary source

04 / THE BRIEF

Scheduled isn't shipped

Cloud Software Group's 24 October statement identifies NetScaler ADC, NetScaler Gateway and TIBCO Fulfillment Provisioning as affected. NetScaler fixes are planned for 27 October; TIBCO remediation is being prepared.

AWS identifies EMR-on-EC2 4.2.0-5.29.0 and 5.30.0-6.15.0 with Ganglia as affected. EMR 7.x, EMR on EKS and EMR Serverless aren't.

PAN-OS/Panorama exposure remains limited to management web interfaces, not GlobalProtect. The 26-30 October hotfix dates remain estimates.

SOURCES

Cloud Software Group Communication Regarding Recent PHP Vulnerabilities - Primary source

PHP web runtimes (CVE-2026-109618 and CVE-2026-109619) - Primary source

Impact of Critical Vulnerabilities in PHP on Palo Alto Networks Products - Primary source

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

05 / THE BRIEF

Fix the running interpreter

PHP's 21 October fixes remain 8.5.12, 8.4.27, 8.3.36 and 8.2.35. Verify full distribution package builds and replace running workers. Forge's automatic security updates exclude PHP.

The separate CVE-2026-115560 vector requires upload progress enabled, php_binary or php_serialize configured, and application code switching to php before session_start(). For that combination, PHP recommends session.upload_progress.enabled=0 until the next regular bugfix release. This isn't a failure of the original fixes.

SOURCES

PHP - Security advisory and informational advisory: Session upload progress - 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

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.