It's Probably Nothing
by Sierra Echo Charlie

SPECIAL EDITION / 24 OCTOBER 2026

Special edition: CVE-2926-109618 (Update #4)

Sophos retracts its compromise report; PHP adds separate, narrowly scoped guidance

6 stories / Listen online - 3:46

THE TAKEAWAY

PHP2Shell still warrants urgent patching; the live-attack evidence is narrower than our last edition reported. Current to 07:04 NZDT on 24 October, or 05:04 AEDT.

01 / THE BRIEF

What changed

Sophos has withdrawn the successful-compromise report carried in Update #3. Its 22 October, 21:21 UTC correction reports scanning and failed attempts, with no evidence of successful compromise in its telemetry. The suspected Potassium/Mirai payload wasn't delivered because the attempt was blocked. That's a correction to our lead, not an all-clear elsewhere.

PHP's 23 October notice adds a separate RCE vector, CVE-2026-115560-not a failure of the original fixes. With upload progress enabled, exposure requires an application configured with the php_binary or php_serialize session handler to switch to php at runtime before session_start(). PHP recommends session.upload_progress.enabled=0 until the next regular bugfix release; applications that never change handlers at runtime can retain the feature.

SOURCES

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

PHP - Informational advisory: Session upload progress - Primary source

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

02 / THE BRIEF

The underlying risk hasn't disappeared

The published identifiers are CVE-2026-109618 and CVE-2026-109619. These PHP-core bugs leave incompletely initialised or freed request state available for later code to consume. PHP puts all web-serving installations in scope.

mod_php has the highest demonstrated risk, including RCE before application code runs. FPM has validated RCE for the second flaw, requiring suitable application behaviour; PHP hasn't demonstrated a complete FPM exploit for the first. Code runs as the web worker, not automatically root.

SOURCES

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

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

03 / THE BRIEF

Keep the earlier investigation window

AWS reports a MadPot exploitation attempt on 17 October, before the 20 October public leak. It doesn't establish success against real systems or how the actor obtained exploit information. Its investigation window still starts from at least 17 October.

VulnCheck now claims commercial exploit support for PHP 8.4.10-8.4.26. That's vendor testing, not proof of portability across arbitrary production deployments.

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

04 / THE BRIEF

Installed isn't necessarily running

PHP released fixes on 21 October: 8.5.12, 8.4.27, 8.3.36 and 8.2.35. Distribution backports can look older; verify the full package build. Minimal source backports exist for 7.4, 8.0 and 8.1 without restoring normal support.

Replace running workers too. Forge's automatic security updates exclude PHP: update every installed version and restart long-running processes. Configuration workarounds don't fully fix the original pair.

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

Supplier fixes aren't interchangeable

Palo Alto Networks limits PAN-OS/Panorama exposure to management web interfaces, not GlobalProtect. Its 26-30 October hotfix dates are estimates, not released fixes. AWS has completed WorkMail's upgrade, but new Lightsail blueprints don't update existing instances.

SOURCES

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

SSA-566512: PHP2Shell Vulnerabilities in Palo Alto Networks PAN-OS on RUGGEDCOM APE1808 Devices - Primary source

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

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

RHSA-2026:88561 - Important: php security update - Primary source

06 / THE BRIEF

Local impact remains unresolved

NZ NCSC says it's too early to determine national impact. Its useful question for providers: were compromise checks done, not just updates? Patching doesn't remove an existing compromise. NZ/AU victim totals remain unresolved.

SOURCES

NCSC urges small businesses to check websites and online services following PHP vulnerability - Primary source

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

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.