21 OCT 2026

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

Critical Remote Code Execution Vulnerabilities in PHP

No Login Needed	Memory Flaws	Attacks Reported	Fixes Available

Executive Summary

The Cal-CSIC has become aware of two critical remote code execution vulnerabilities, CVE-2026-109618 and CVE-2026-109619, affecting PHP installations serving web requests. Each vulnerability carries a CVSS 4.0 score of 9.2, according to the PHP security team. Apache with mod_php faces the highest assessed risk; PHP FastCGI Process Manager (PHP-FPM), php-cgi, FrankenPHP and LiteSpeed deployments also require assessment.[1, 2, 3]

CVE-2026-109618 involves out-of-memory error handling that can leave request data partially initialized and unsafe for cleanup. CVE-2026-109619 involves request-owned state surviving after its backing memory is freed; another request handled by the same worker can consume that stale state. Successful exploitation allows an unauthenticated attacker to execute code with the web worker's privileges. Exploit reliability depends on the build, configuration and memory layout; no user interaction is required.

The PHP project released fixes on October 21, 2026. Configuration workarounds address only specific paths and do not fully remediate either vulnerability. Open-source reporting describes exploitation observed by a honeypot network on October 21, 2026. Public exploit demonstrations and technical analysis are available; a public repository also advertises proof-of-concept (PoC) code for CVE-2026-109618, whose reliability has not been independently validated for this advisory.[4, 5, 6]

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Recommended Actions

The Cal-CSIC recommends that clients immediately update affected PHP runtimes, prioritizing internet-facing web servers, and restart all affected web and PHP worker processes so patched code is loaded. Clients using distribution or long-term support packages should confirm a vendor backport covering both CVEs. If updating is delayed, apply the PHP project's partial mitigations while expediting the upgrade. Review web-worker activity for unexpected command execution and escalate suspected compromise through established incident response procedures.

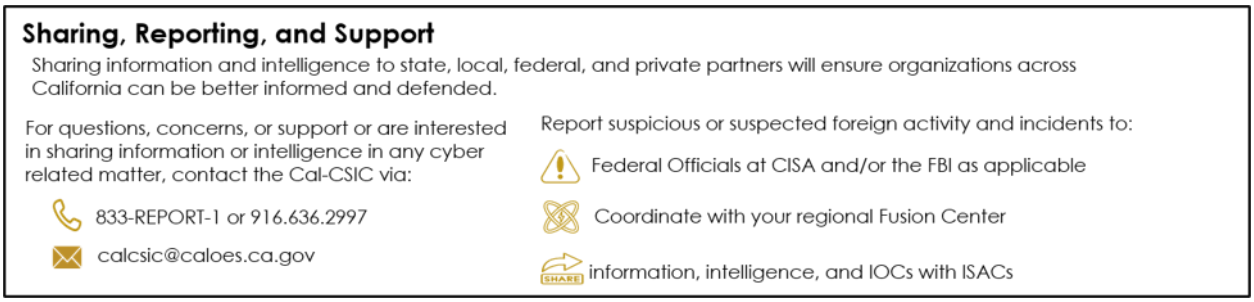
Affected Releases and Updated Version

Affected Product	Affected Range	Updated Version
PHP 8.5	**Earlier than 8.5.12**	**8.5.12**
PHP 8.4	**Earlier than 8.4.27**	**8.4.27**
PHP 8.3	**Earlier than 8.3.36**	**8.3.36**
PHP 8.2	**Earlier than 8.2.35**	**8.2.35**
PHP 8.1 and Older	**Affected legacy deployments**	**Upgrade or obtain a vendor backport**

Both CVEs are addressed by the fixed versions above. Legacy branches do not receive regular upstream PHP security releases; limited source backports exist for PHP 7.4, 8.0 and 8.1. Confirm coverage with the package vendor.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

Sharing, Reporting, and Support



References:

[1] PHP Group; “Security advisory: Critical remote code execution vulnerabilities, update now"; https://www.php.net/archive/2026.php; accessed October 21, 2026.
[2] PHP Group; “RCE via OOM corruption”; https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w; accessed October 21, 2026.
[3] PHP Group; “RCE via stale global state”; https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp; accessed October 21, 2026.
[4] watchTowr; “Frequently Asked Questions About PHP Remote Code Execution”; https://watchtowr.com/intelligence/php-cve-2026-109618-faq/; accessed October 21, 2026.
[5] Calif Research; “A tale of two PHP remote vulnerabilities”; https://calif.io/php2shell/; accessed October 21, 2026.
[6] eness; "php2shell public PoC repository (code availability only)"; https://github.com/eness/php2shell-CVE-2026-109618-CVE-2026-109619-PoC), accessed October 21, 2026.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.