GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

16 November 2026

Advisory 378: PHP2Shell Remote Code Execution Vulnerabilities Actively Exploited (CVE-2026-109618 and CVE-2026-109619).

Release Date: 13th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

The PHP project published a security release on 21 October 2026 (14:00 UTC, which was 01:00 on 22 October in Vanuatu) that fixes two critical remote code execution (RCE) vulnerabilities in the PHP core. This advisory updates CERTVU Advisory 365 of 22 October 2026, because both flaws are now actively exploited. Both flaws are rated CVSS v4.0 9.2 (Critical), with a network attack vector, no privileges required and high attack complexity, and the same five weaknesses are listed for each: CWE-416 (use after free), CWE-755, CWE-824, CWE-1325 and CWE-1419.

CVE-2026-109618 is an RCE through out-of-memory (OOM) corruption. PHP uses longjmp() to handle out-of-memory errors. If an allocation fails while request memory is only partly initialized, the early exit leaves invalid internal state, and request cleanup then treats it as valid. Oversized or malformed multipart requests are one way to reach the out-of-memory condition. The PHP advisory states the confirmed impact is unauthenticated RCE as the web worker account, validated against mod_php with default settings, where an unauthenticated request triggers the attack before any application code runs.

CVE-2026-109619 is an RCE through stale global state. A persistent PHP worker can keep request-owned internal state that points to memory freed after a previous request. Fatal errors, including out-of-memory errors and execution timeouts, or diagnostics emitted during shutdown can leave this

state unreset, and a later request on the same worker may use it before normal initialization, causing a use-after-free. Confirmed early users of the stale state are INI diagnostics and session upload progress handling, and the PHP 8.5 fatal_error_backtraces feature is the confirmed RCE path against mod_php.

What are the systems affected?

All PHP installations that serve web requests are affected before the fixed releases, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. The risk is highest for mod_php. The following versions are affected:

- PHP 8.5 before 8.5.12
- PHP 8.4 before 8.4.27
- PHP 8.3 before 8.3.36
- PHP 8.2 before 8.2.35 (PHP 8.2 reaches end of life on 31 December 2026)
- PHP 8.1 and older, which no longer receive releases from the PHP project, including PHP 7.4 and 8.0. Earlier PHP 5 and 7 versions are reported as possibly affected
- Pre-release builds of PHP 8.6.0 before 8.6.0 RC4
- Applications running on PHP, such as WordPress, Joomla and Drupal sites, depend on the PHP version of the host

Not affected / patched version:

- PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or later
- PHP 8.6.0 RC4 for the pre-release branch
- For PHP 7.4, 8.0 and 8.1, the PHP security team published minimal source backports as branches in the php-src repository. Some distributions and long-term support vendors also provide backported fixes, so check with your vendor. Where no fix is available, upgrade to a supported branch

What does this mean?

Successful exploitation may allow attackers to:

- Send a request that triggers the flaw before any application code runs, and run code on the server as the web worker account without logging in (confirmed for mod_php)
- Install web shells, steal data and credentials held by the web application, and deface or disrupt hosted sites
- Use the compromised web server as a foothold into the hosting network

Mitigation process

CERTVU recommends the following:

Update PHP
Update every PHP installation to 8.5.12, 8.4.27, 8.3.36, 8.2.35 or later, and restart PHP-FPM, Apache and other workers so the new version is running. Shared hosting providers usually apply updates, so ask them when they will deploy. Upgrade PHP 8.1 and older to a supported branch, or apply the security team's backport or a vendor backport. PHP states that only updating is a complete fix.

Reference

1. https://www.php.net/
2. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
3. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
4. https://www.cyber.gov.au/alert/critical-vulnerabilities-in-php
5. https://www.helpnetsecurity.com/2026/10/21/php-security-release-announcement-october-2026/
6. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
7. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-109618
8. https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-109619