An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2610210276

NCSC Advisory

PHP Critical Vulnerabilities

CVE-2026-109618 & CVE-2026-109619

21st, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Published: 2026-21-10

Vendor: PHP Foundation

Product: PHP

CVE ID:

- CVE-2026-109618
    - RCE via OOM corruption, CVE-2026-109618 (GHSA-w8hw-w9fx-j79w): out-of-memory handling can interrupt PHP while internal request data is only partially initialized. Request cleanup may then treat the invalid data as valid.
    - **Common Weakness Enumeration (CWE)[1]:**
        - **CWE-416 Use after free,**
        - **CWE-755 Improper Handling of Exceptional Conditions,**
        - **CWE-824 Access of uninitialized pointer,**
        - **CWE-1325 Improperly controlled sequential memory allocation,**
        - **CWE-1419 Incorrect Initialization of Resource**
    - Known Exploited Vulnerability (KEV) catalog[2]: No
    - Used by Ransomware Operators: N/A
- **CVSS Score[3]:** 9.2

- CVE-2026-109619
    - RCE via stale global state, CVE-2026-109619 (GHSA-6wmf-4rv5-p3rp): request-owned internal state can survive after its backing memory has been freed. A later request handled by the same worker may use that stale state before normal initialization resets it.
    - **Common Weakness Enumeration (CWE):**
        - CWE-416 Use after free,
        - CWE-755 Improper Handling of Exceptional Conditions,
        - CWE-824 Access of uninitialized pointer,
        - CWE-1325 Improperly controlled sequential memory allocation,

[1] https://cwe.mitre.org
[2] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[3] https://www.first.org/cvss/

        - CWE-1419 Incorrect Initialization of Resource
    - Known Exploited Vulnerability (KEV) catalog: No
    - Used by Ransomware Operators: N/A
- **CVSS Score:** 9.2

Products Affected

All PHP installations serving web requests, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. The PHP Foundation consider the risk highest for mod_php, with a demonstrated exploit where an unauthenticated request can trigger the attack before any application code runs.

Product	Version
PHP	8.2.* < 8.2.35
PHP	8.3.* < 8.3.36
PHP	8.4.* < 8.4.27
PHP	8.5.* < 8.5.12

Impact

PHP (PHP Hypertext Preprocessor) is a widely used server-side scripting language designed for web development. It runs on a web server to generate dynamic page content, interact with databases, and handle backend application logic before delivering the final HTML output to a user's browser. PHP is also used in a range of other products.

Two critical RCE CVEs - CVE-2026-109618, CVE-2026-109619 have been published today. All organisations are advised to identify all php installations in their networks and infrastructure - this means any php installation that is contained within vendor software in addition to the PHP version being utilised in their own configurations. Once your list is complete:

1. Focus on patching your internet facing instances first, then patch your other instances
2. Identify any EOL version of PHP within your estate and isolate them, if mitigations cannot be applied.

(PHP currently supports 8.2,8.3,8.4 and 8.5 branches, all version of PHP below 8.2 are EOL)

In addition to the above some applications and versions of PHP may not be served via the main PHP respositories and so patches may take time to filter through this should be taken into account in your attempts to mitigate these vulnerabilities.

NB: All versions of PHP prior to PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35 are affected.

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from PHP.

https://www.php.net/archive/2026.php#2026-10-20-1

NCSC-NL have provided further information on software with a PHP dependency that may be potentially affected by the vulnerabilities: https://github.com/NCSC-NL/php2shell