An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611200238

NCSC Advisory

Multiple Critical Vulnerabilities in PHP

20 November 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

Multiple vulnerabilities in PHP affect session handling, error processing, and HTTP request handling in PHP-FPM. Depending on the vulnerability and server configuration, a remote attacker could execute arbitrary code, cause a denial of service, or smuggle HTTP requests to the backend.

Products Affected

CVE ID	Product	Version
CVE-2026-115560 CVE-2026-126714 CVE-2026-129289 CVE-2026-129496	PHP	0 < 8.2.36 8.3.0 < 8.3.37 8.4.0 < 8.4.28 8.5.0 < 8.5.13
CVE-2026-129474 CVE-2026-129182	PHP	8.5.0 < 8.5.13
CVE-2026-129481	PHP	8.3.0 < 8.3.37 8.4.0 < 8.4.28 8.5.0 < 8.5.13

CVE Details

CVE ID: CVE-2026-115560

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score[1]: 9.2

Common Weakness Enumeration (CWE)[2]: CWE-20 Improper Input Validation, CWE-502 Deserialization of Untrusted Data

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-126714

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score: 9.2

Common Weakness Enumeration (CWE): CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition, CWE-662: Improper Synchronization

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

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

CVE ID: CVE-2026-129289

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score: 9.2

Common Weakness Enumeration (CWE): CWE-444: Inconsistent Interpretation of HTTP Requests, CWE-670: Always-Incorrect Control Flow Implementation

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-129496

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score: 9.2

Common Weakness Enumeration (CWE): CWE-416: Use After Free, CWE-459: Incomplete Cleanup

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-129474

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score: 9.2

Common Weakness Enumeration (CWE): CWE-416: Use After Free

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-129182

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score: 9.2

Common Weakness Enumeration (CWE): CWE-416: Use After Free, CWE-459: Incomplete Cleanup

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

CVE ID: CVE-2026-129481

Published: 2026-11-19

Vendor: PHP Group

Product: PHP

CVSS Score: 9.2

Common Weakness Enumeration (CWE): CWE-416 Use After Free, CWE-459 Incomplete Cleanup

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

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 the PHP Group.

References

CVE-2026-115560

- https://nvd.nist.gov/vuln/detail/CVE-2026-115560
- https://www.cve.org/CVERecord?id=CVE-2026-115560
- https://github.com/php/php-src/security/advisories/GHSA-658j-r8rw-q6mx

CVE-2026-126714

- https://nvd.nist.gov/vuln/detail/CVE-2026-126714
- https://www.cve.org/CVERecord?id=CVE-2026-126714
- https://github.com/php/php-src/security/advisories/GHSA-fm2m-fjf5-v3cp
- https://github.com/semgrep/detection-scripts/pull/14
- https://depthfirst.com/research/phpaftershell
- https://bugzilla.suse.com/show_bug.cgi?id=1290690
- https://ubuntu.com/security/CVE-2026-126714

CVE-2026-129289

- https://nvd.nist.gov/vuln/detail/CVE-2026-129289
- https://www.cve.org/CVERecord?id=CVE-2026-129289
- https://github.com/php/php-src/security/advisories/GHSA-qc49-hpvq-g2w6
- https://github.com/anonaddy/docker/issues/465
- https://bugzilla.suse.com/show_bug.cgi?id=1290687
- https://ubuntu.com/security/CVE-2026-129289

CVE-2026-129496

- https://nvd.nist.gov/vuln/detail/CVE-2026-129496
- https://www.cve.org/CVERecord?id=CVE-2026-129496
- https://github.com/php/php-src/security/advisories/GHSA-gr4f-wgx5-jpfv

CVE-2026-129474

- https://nvd.nist.gov/vuln/detail/CVE-2026-129474
- https://www.cve.org/CVERecord?id=CVE-2026-129474
- https://github.com/php/php-src/security/advisories/GHSA-8mjj-2r7p-4hg2

CVE-2026-129182

- https://nvd.nist.gov/vuln/detail/CVE-2026-129182
- https://www.cve.org/CVERecord?id=CVE-2026-129182
- https://github.com/php/php-src/security/advisories/GHSA-2fjv-p558-g82m

CVE-2026-129481

- https://nvd.nist.gov/vuln/detail/CVE-2026-129481
- https://www.cve.org/CVERecord?id=CVE-2026-129481
- https://github.com/php/php-src/security/advisories/GHSA-g3vh-838c-65v7