



Security Advisory 2026-018

Critical Vulnerabilities in PHP

2026-10-21 — v1.0

TLP:CLEAR

History:

- 21/10/2026 — v1.0 – Initial publication

Summary

On 20 October 2026, the PHP foundation announced an upcoming security release addressing two critical vulnerabilities in PHP that could lead to remote code execution, according to other leaks [1,2,3].

At this time, no technical details have been made public. CERT-EU advises organisations to prepare for **immediate patching of affected assets**. Where immediate patching is not feasible, organisations should **consider isolating internet-facing applications from public networks until a fix is available**.

The PHP team has scheduled the release for 21 October 2026 at 14:00 UTC [1].

Technical Details

No technical details are currently available for **CVE-2026-109618** and **CVE-2026-109619**, apart from their CVSS scores of 9.2, which indicate the potential for unauthenticated remote code execution [1].

Affected Products

These vulnerabilities could affect all PHP versions from PHP 5 onwards [2].

Recommendations

CERT-EU strongly recommends identifying PHP-based applications and preparing to **patch as soon as fixed versions become available**. Where immediate remediation is not feasible, organisations should **consider isolating internet-facing applications from public networks until a fix can be applied**.

References

- [1] <https://www.php.net/archive/2026.php#2026-10-20-1>
- [2] <https://cyberplace.social/@GossiTheDog/117474220875882526>
- [3] <https://x.com/watchtowrcyber/status/2112611507749982605>