CERT-EU: Critical PHP Flaws Allow Unauthenticated Remote Code Execution; Patch Now



CERT-EU reports two critical PHP vulnerabilities enabling unauthenticated remote code execution, fixed in 8.5.12, 8.4.27, 8.3.36 and 8.2.35. Proofs of concept are circulating, and a third RCE flaw has a mitigation only.

- CVE-2026-109618 and CVE-2026-109619, both CVSS 9.2, can allow unauthenticated remote code execution.
- Fixed in PHP 8.5.12, 8.4.27, 8.3.36 and 8.2.35; PHP 8.1 and older receive no project updates.
- Technical details are public and proofs of concept are circulating, so exploitation may already be under way.
- A third RCE, CVE-2026-115560, affects only unusually configured web applications; no out-of-band release is planned.

> - All PHP setups serving web requests are at risk, with mod_php considered the highest-risk setup.

What happened

On 20 October 2026 the PHP project announced a security release for two critical flaws, and the fixes were published on 21 October. CERT-EU notes that both can allow unauthenticated remote code execution, that technical details are being discussed publicly and that initial proofs of concept have begun to circulate. This raises the likelihood that attackers are already exploiting them.

CVE-2026-109618 involves memory corruption when PHP aborts a request that exceeds its memory limit, which can leave request data partly initialised. **CVE-2026-109619** involves stale internal state surviving after its memory is freed and being reused by a later request in the same worker. A demonstrated exploit shows a single unauthenticated request can trigger the attack before any application code runs.

On 23 October PHP disclosed a third RCE, CVE-2026-115560. It affects only web applications configured in an unusual way, PHP considers it unlikely, and no out-of-band release will be issued. Full details will come with the next release.

Who is affected

Any PHP installation serving web requests is at risk, including PHP-FPM, Apache with mod_php, php-cgi, FrankenPHP and LiteSpeed. Branches earlier than 8.5.12, 8.4.27, 8.3.36 and 8.2.35 are affected, as are end-of-life versions. Commercial and open-source products that embed PHP may also be affected even if PHP is not directly exposed. CERT-EU points to the NCSC-NL repository for identifying such software.

Recommended response

Update to a fixed version immediately, or obtain patched packages from your distribution or LTS vendor. If patching is not feasible, consider isolating internet-facing applications from public networks until the fix is applied and verified. Temporary configuration measures only reduce exposure to specific attack paths and do not make an installation safe. For CVE-2026-115560, disabling session.upload_progress.enabled and restarting all workers is the advised protection until the next regular release.

What to do now

1. Inventory all internet-facing PHP applications and the PHP versions and server modes (mod_php, PHP-FPM and others) they run.
2. Upgrade to PHP 8.5.12, 8.4.27, 8.3.36 or 8.2.35, or obtain patched packages from your distribution or LTS vendor, and verify the result.
3. Plan migration or vendor-backported fixes for PHP 8.1 and older, which receive no project updates.
4. Ask vendors of third-party products whether they embed PHP, using the NCSC-NL repository as a

reference.

5. Where patching must wait, isolate exposed applications from public networks and apply the documented temporary mitigations, treating them as partial only.
6. Set session.upload_progress.enabled=0 in server-level configuration, restart all workers, and review web and WAF logs for anomalous unauthenticated requests.