Critical security issue affecting PHP

The NCSC is encouraging UK organisations to take immediate action to mitigate a security issue affecting PHP (CVE-2026-109618 and CVE-2026-109619).

What has happened?

PHP has published a security update to address a critical security issue that may allow attackers to execute commands on any web server running PHP.

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.

The security issue could allow an attacker to trigger an out-of-memory (OOM) condition in PHP that results in memory corruption. Under certain conditions, this corruption could be exploited to achieve unauthenticated remote code execution. This security issue has now been fixed.

- **CVE-2026-109618:** 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.
- **CVE-2026-109619:** 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.

The full PHP security advisory provides more details regarding the fixed security issue.

The NCSC will continue to monitor for any impact on UK organisations.

Who is affected?

Organisations using any version of PHP are affected and all organisations are highly encouraged to update to the latest fixed version. Organisations using older versions of PHP are highly encouraged to update to a fully supported version.

What should I do?

The NCSC recommends following vendor best practice advice in the mitigation of vulnerabilities. The NCSC highly encourages organisations to follow these priority actions:

1. Identify systems running PHP across your infrastructure, prioritising internet-facing systems. As all versions may be affected, do not limit discovery to outdated PHP versions; identify PHP installations generally and assess their exposure to CVE-2026-109618 and CVE-2026-109619.
2. Update to the latest version of PHP and continue to monitor for future updates.
3. If you are unable to update to a version with the security update applied, the PHP Foundation have provided temporary mitigations.
4. If you are unable to apply the temporary mitigations, or applying them would take too long, you should consider taking the system offline until it can be fully mitigated.
5. If you are unable to update or disable the system immediately then you should assess the system for any evidence of compromise prior to your upgrade or mitigation and look for backdoors installed by an attacker. If you are not confident in your ability to do this yourselves then you can get assistance from an NCSC-assured Cyber Incident Response provider.
6. Continuously monitor for security updates from third-party software vendors, including for appliances and services that may bundle PHP. NCSC-NL have published an inventory list of software products with a PHP dependency potentially affected by the vulnerabilities. Apply relevant updates as they become available.

Further NCSC resources

- NCSC blog post: Preparing for a 'vulnerability patch wave'
- Follow NCSC guidance including vulnerability management and preventing lateral movement
- NCSC principles secure build and deployment pipelines
- If your organisation is in the UK, you can sign up to the free NCSC Early Warning service to receive notifications of potential threats on your network
- The NCSC Vulnerability Disclosure Toolkit helps organisations of all sizes with the essential components of implementing a vulnerability disclosure process

PUBLISHED

21 October 2026

NEWS TYPE

Alert