Critical security issue affecting PHP

The NCSC is encouraging UK organisations to prepare for immediate updating of systems using PHP.

The NCSC is encouraging UK organisations to prepare for immediate updating of systems using PHP. Where immediate remediation is not feasible, organisations should consider taking the system offline until it can be fully mitigated.

The release is scheduled for Wednesday, 21 October 2026 at 15:00 BST, but may occur earlier. This page will also be updated.

Organisations should:

1. Identify systems running any version of PHP across your infrastructure, prioritising internet-facing systems
2. Perform monitoring of internet-facing PHP systems for malicious activity
3. Monitor the PHP official guidance
4. Apply PHP updates as they become available
5. Continuously monitor for security updates from third-party software vendors, including for appliances and services that may bundle PHP

Background

On 20 October 2026, the PHP Foundation announced an upcoming security release addressing two critical vulnerabilities in 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.

PUBLISHED

21 October 2026

NEWS TYPE

Alert