



CYBERSECURITY ADVISORY

PHP2Shell Critical Remote Code Execution Vulnerabilities in PHP

Severity: Critical | CVSS v4.0: 9.2

Vulnerabilities: CVE-2026-109618 and CVE-2026-109619

Overview

All organisations and individuals in Kenya operating systems built on PHP are advised to urgently identify affected installations and apply the security updates. This includes public institutions, county governments, businesses, critical infrastructure operators, educational institutions, developers and hosting providers. The advisory covers systems operated directly or managed by third parties, including cloud and hosted environments.

Two critical PHP vulnerabilities could allow unauthenticated remote code execution, compromising application data and disrupting services. The flaws involve memory corruption during out-of-memory handling and the reuse of invalid internal state between requests.

PHP installations serving web requests require urgent attention, including PHP-FPM, Apache mod_php, php-cgi, FrankenPHP and LiteSpeed. PHP identifies Apache mod_php as particularly exposed, with demonstrated exploitation before application code runs.

Affected and fixed versions

PHP branch	Affected versions	Fixed version
8.2	Earlier than 8.2.35	8.2.35
8.3	Earlier than 8.3.36	8.3.36
8.4	Earlier than 8.4.27	8.4.27
8.5	Earlier than 8.5.12	8.5.12

PHP 8.1 and older no longer receive routine upstream security updates. Organisations using these versions should migrate to a supported release or obtain explicit confirmation of backported fixes from their distribution or support provider.

Recommended actions

1. Apply the appropriate security update immediately, prioritising internet-facing websites, portals and APIs.
2. Identify PHP installations across websites, portals, internal applications, servers, containers and hosting platforms. Require hosting providers and vendors to confirm affected systems and patch completion.
3. Restart affected PHP workers and relevant services after updating. Verify the runtime actually serving each application.
4. Where immediate patching is not possible, consider temporarily isolating affected applications from public access. Configuration changes provide only partial protection; updating is the complete remedy.
5. Review logs, web directories, running processes and outbound connections for suspicious activity. Preserve relevant evidence and activate incident response procedures where compromise is suspected.

Updating a content management system or its plugins alone does not replace patching the underlying PHP runtime.

Reference

PHP official security advisory <https://www.php.net/archive/2026.php#2026-10-21-5>