



URGENT ADVISORY: CRITICAL PHP2SHELL VULNERABILITIES REQUIRE IMMEDIATE PATCHING

Dear Stakeholders,

The Botswana National Computer Security Incident Response Team (CSIRT) issues this urgent advisory regarding two critical vulnerabilities in the PHP runtime, identified as CVE-2026-109618 and CVE-2026-109619, collectively referred to as PHP2Shell. These vulnerabilities affect PHP- based websites, portals and applications and may expose organisations to remote code execution and sensitive information disclosure.

The vulnerabilities affect PHP versions 5.4 through 8.5.11 across web- serving environments, including PHP-FPM, Apache mod_php, php-cgi, FrankenPHP and LiteSpeed. Websites built using platforms such as WordPress, Drupal, Joomla, Magento, Laravel and custom PHP applications may also be affected when running a vulnerable PHP runtime. Exploitation attempts have been observed, and organisations should treat internet-facing PHP servers as vulnerable until the runtime version has been verified and patched.

Immediate Actions Required:

- Identify all systems running PHP, including internet-facing servers, containers, development and staging environments, and third-party or managed hosting services.
- Update PHP immediately to a fixed release or newer: 8.5.12, 8.4.27, 8.3.36 or 8.2.35, as applicable.
- Restart Apache, PHP-FPM and all long-running PHP workers after applying updates to ensure the patched runtime is active.
- Review web server, PHP and PHP-FPM logs for unusual requests, repeated HTTP 500 errors, memory-limit errors, unexpected worker crashes or restarts.
- Investigate signs of possible compromise, including unfamiliar PHP files, web server processes launching shells or network tools, unexpected outbound connections, and unrecognised accounts or scheduled tasks.
- Where exposure or compromise is suspected, rotate potentially affected passwords, API keys and application secrets, invalidate active sessions, and review administrator accounts.
- Contact hosting providers, application vendors and third-party developers to confirm that affected systems have been patched. Temporary mitigations and web application firewall rules do not replace updating PHP.

Organisations that suspect exploitation or require assistance identifying exposed systems are urged to notify the National CSIRT through established reporting channels. Organisations that do not use PHP are not affected by this advisory.

Your vigilance and cooperation are essential in safeguarding Botswana's digital ecosystem.

