

AUTORIDADE REGULADORA DE TIC

Alerta de Segurança

Vulnerabilidades críticas do PHP (PHP2Shell)

No dia 21 de outubro de 2026, o projecto PHP divulgou duas vulnerabilidades críticas no próprio PHP, conhecidas como «PHP2Shell»: CVE-2026-109618 e CVE-2026-109619 (CVSS 9,2). Estas vulnerabilidades podem permitir a execução remota de código sem autenticação através de pedidos web manipulados, independentemente da aplicação que esteja a ser executada. O projeto PHP afirma que todas as instalações do PHP que atendem a pedidos web estão em risco:

- PHP-FPM,
- Apache com mod_php,
- php-cgi,
- FrankenPHP e
- LiteSpeed.

O risco é maior no Apache com mod_php. Os fornecedores de segurança relataram as primeiras tentativas de exploração.

Recomendações

- Actualize o PHP para a versão 8.2.35, 8.3.36, 8.4.27 ou 8.5.12 ou posterior, ou para o pacote corrigido da sua distribuição Linux (as distribuições podem manter o número da versão antiga). Em seguida, reinicie o PHP-FPM / Apache para que todos os *workers* executem o código corrigido;
- O PHP 8.1 e versões anteriores chegaram ao fim do ciclo de vida e não recebem lançamentos oficiais. O projecto PHP publicou backports do código-fonte para as versões 7.4, 8.0 e 8.1, e algumas distribuições e fornecedores de LTS disponibilizam correções. Caso contrário, actualize para um ramo suportado;
- Se não for possível actualizar imediatamente, os avisos de segurança indicam configurações provisórias, tais como ``memory_limit=-1`` e ``session.upload_progress.enabled=0`` (no ficheiro ``php.ini`` ou na configuração do servidor, em seguida, reinicie os *workers*). Estas configurações reduzem a exposição à vulnerabilidade, mas não constituem uma correção; o projeto PHP afirma que a actualização é a única medida de mitigação completa.

Maputo, 22 de Outubro de 2026