AVIS DE SECURITE

Objet	**Vulnérabilités critiques d'exécution de code arbitraire à distance dans PHP (CVE-2026-109618, CVE-2026-109619)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-266
TLP	WHITE

Résumé

Le PHP Security Team a publié le 21/10/2026 les versions 8.5.12, 8.4.27, 8.3.36 et 8.2.35 corrigeant deux vulnérabilités critiques du cœur de PHP, surnommées « php2shell » (CVE-2026-109618 et CVE-2026-109619, CVSS v4.0 9.2). La première provient d'une corruption de la mémoire de requête lors du traitement des erreurs de dépassement de mémoire (OOM), déclenchable via des requêtes multipart malveillantes ; la seconde d'un état global obsolète conservé par les workers persistants après la libération de la mémoire associée (use-after-free). Un attaquant non authentifié peut ainsi exécuter du code arbitraire à distance avec les privilèges du processus web, sur toute installation PHP servant des requêtes web, le risque étant maximal avec Apache mod_php où l'attaque intervient avant l'exécution du code applicatif.

Des preuves de concept fonctionnelles ont été démontrées contre WordPress, Drupal et Joomla et des premières tentatives d'attaque sont signalées. La CISA appelle à l'application immédiate des correctifs. Les branches PHP 8.1 et antérieures, en fin de vie, sont également vulnérables et ne bénéficient pas de correctif officiel.

Risque de sécurité

- Exécution de code arbitraire à distance sans authentification
- Atteinte à la confidentialité des données (divulgation de la mémoire des processus PHP)
- Atteinte à l'intégrité des données et compromission des applications web hébergées
- Déni de service

Systèmes affectés

- PHP 8.5.x versions antérieures à 8.5.12
- PHP 8.4.x versions antérieures à 8.4.27
- PHP 8.3.x versions antérieures à 8.3.36
- PHP 8.2.x versions antérieures à 8.2.35
- PHP 8.1 et versions antérieures (en fin de vie, sans correctif officiel)
- Toutes les installations servant des requêtes web : PHP-FPM, Apache mod_php, php-cgi, FrankenPHP, LiteSpeed

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 21/10/2026 et mettre à jour sans délai vers PHP 8.5.12, 8.4.27, 8.3.36 ou 8.2.35 (ou vers les paquets corrigés fournis par les distributions Linux), puis redémarrer l'ensemble des workers PHP. La mise à jour est la seule mesure corrective complète ;
2. A défaut d'une mise à jour immédiate, appliquer les mesures temporaires de réduction d'exposition décrites par l'éditeur (notamment session.upload_progress.enabled=0, limitation de post_max_size et de la taille des requêtes, fatal_error_backtraces=0 sous PHP 8.5) :

    - https://www.php.net/archive/2026.php#2026-10-21-5
    - https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
    - https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
    - https://www.php.net/ChangeLog-8.php
    - https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar
https://www.stcc-ssi.sn/

E-mail : sncsirt@dcssi.sn

Date de publication : 21/10/2026