

ALERTE CRITIQUE

PHP : deux failles critiques permettent de prendre le contrôle d'un serveur web

CVE-2026-109618 · CVE-2026-109619

9,2

SCORE CVSS 4.0 DE L'ÉDITEUR PHP, LE PLUS ÉLEVÉ SUR 10

RÉFÉRENCE

UNIDEES-CSIRT-221026-001

VERSION

v1.2

CLASSIFICATION

Public

PUBLICATION

22/10/2026, mise à jour le
26/10/2026

IDENTIFICATION

21/10/2026

SOURCES

Projet PHP (php.net), CVE, CISA ;
Rapid7 en complément

RÉSUMÉ

Le 21 octobre 2026, le projet PHP a publié des correctifs pour deux vulnérabilités qui permettent **d'exécuter du code à distance, sans authentification**, sur un serveur qui fait tourner PHP. Point à J+5 (26/10/2026) : les correctifs restent disponibles et la mise à jour reste la seule mesure complète.

FICHE

VULNÉRABILITÉS

CVE-2026-109618 et CVE-2026-109619

GRAVITÉ

Critique : CVSS 4.0 à 9,2 pour les deux (éditeur PHP et enregistrements CVE)

IMPACT

Exécution de code à distance, sans authentification

EXPLOITATION

Non inscrites au catalogue des vulnérabilités exploitées de la CISA (version du 23/10/2026)

CORRECTIF

Disponible depuis le 21/10/2026

RISQUES DE SÉCURITÉ

- Exécution de code à distance, sans authentification
- Prise de contrôle du serveur web et des applications qu'il héberge
- Selon Rapid7 (complément) : CVE-2026-109618, corruption de mémoire lors d'une gestion de mémoire épuisée ; CVE-2026-109619, état global valable après libération de la mémoire

QUI EST CONCERNÉ

Toute installation PHP qui sert des pages web est concernée, quel que soit le système : PHP-FPM, Apache avec mod_php, php-cgi, FrankenPHP et LiteSpeed. Le projet PHP juge le risque **le plus élevé pour mod_php**, où une simple requête non authentifiée peut déclencher l'attaque avant même l'exécution du code de l'application. Sont donc exposés les sites, les CMS (WordPress, Drupal...) et les applications métier écrites en PHP.

VERSIONS CORRIGÉES

PHP 8.2	8.2.35
PHP 8.3	8.3.36
PHP 8.4	8.4.27
PHP 8.5	8.5.12
PHP 8.1 et antérieures	pas de version corrigée : migrer

CONTOURNEMENT

Aucun contournement complet selon le projet PHP : la mise à jour est la seule mesure sûre. Mesure intérimaire selon l'avis du projet PHP du 23/10/2026 : `session.upload_progress.enabled = 0` jusqu'à la prochaine version de correction ; elle ne protège pas contre CVE-2026-109618. Sous PHP 8.5 : `fatal_error_backtraces = 0` (php.net).

CE QU'IL FAUT FAIRE

01 Mettre à jour maintenant

Passer en 8.2.35, 8.3.36, 8.4.27 ou 8.5.12, puis **redémarrer tous les processus PHP** (FPM, Apache).

02 Traiter les versions 8.1 et antérieures

Le projet PHP ne publie plus de version corrigée pour ces branches ; il a seulement mis à disposition des correctifs minimaux en code source pour PHP 7.4 à 8.1. Planifier la migration vers une version maintenue ou appliquer le correctif de la distribution, et isoler ces serveurs d'ici là.

03 En attendant, réduire l'exposition

Appliquer les mesures partielles ci-dessus. Elles ne remplacent pas la mise à jour.

04 Surveiller

Rechercher dans les journaux les erreurs PHP inhabituelles et les redémarrages de processus depuis le 21/10, et suivre les avis de l'éditeur PHP.

Besoin d'aide pour évaluer votre exposition ?

Le CSIRT d'UNIDEES accompagne les organisations : inventaire des serveurs exposés, mise à jour, recherche de traces de compromission. Le CSIRT et le SOC managé d'UNIDEES sont certifiés ISO/IEC 27001:2022. Contact : commercial@unidees.dz

SOURCES OFFICIELLES

- php.net · avis de sécurité du 21/10/2026
<https://www.php.net/archive/2026.php#2026-10-21-5>
- php.net · avis informatif du 23/10/2026
<https://www.php.net/archive/2026.php>

- CVE · CVE-2026-109618
<https://www.cve.org/CVERecord?id=CVE-2026-109618>
- CVE · CVE-2026-109619
<https://www.cve.org/CVERecord?id=CVE-2026-109619>
- CISA · catalogue KEV, version du 23/10/2026
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- Rapid7 · analyse technique (complémentaire)
<https://www.rapid7.com/blog/post/etr-cve-2026-109618-and-cve-2026-109619-critical-unauthenticated-remote-code-execution-in-php/>

Informations au 22/10/2026, mise à jour le 26/10/2026. La situation évolue : se reporter aux sources pour la dernière version.