DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 22-11-2026

BULLETIN ALERTES

Object	Vulnérabilité de request smuggling dans PHP-FPM (corps de requête non lu)
Réference	1518
Date de Publication	2026-11-19
Sévérité	Critique

IMPACT :

- Exécution de code PHP à distance non authentifiée
- Contournement des contrôles de routage du frontal web et exécution de code avec les privilèges du worker PHP-FPM

SYSTÉME AFFECTÉ :

- PHP versions antérieures à 8.2.36, 8.3.37, 8.4.28 et 8.5.13 (branches 8.2, 8.3, 8.4 et 8.5)
- Déploiements PHP-FPM (ou LSAPI) derrière un frontal (nginx, Apache, HAProxy) configuré pour réutiliser les connexions backend (ex. nginx avec fastcgi_keep_conn on, Apache mod_proxy_fcgi avec enablereuse=on)

DÉSCRIPTION :

Une vulnérabilité de request smuggling a été identifiée dans PHP-FPM. PHP ne vide pas la partie non lue du corps d'une requête HTTP à la fin de la requête lorsque l'application a ouvert php://input sans le lire jusqu'à la fin. Lorsque le frontal réutilise les connexions backend (configuration non par défaut sous nginx ou Apache), PHP-FPM peut interpréter les octets restants comme une nouvelle requête FastCGI. Un attaquant distant non authentifié peut ainsi forger une requête backend avec des paramètres choisis (SCRIPT_FILENAME, REMOTE_ADDR, PHP_ADMIN_VALUE, etc.), conduisant à l'exécution de code PHP contrôlé par l'attaquant avec les privilèges du worker. Des preuves de concept existent. Aucune exploitation active à grande échelle n'est confirmée par les sources officielles à la date de ce bulletin.

SOLUTION :

Mettre à jour PHP vers les versions corrigées : **8.2.36**, **8.3.37**, **8.4.28** ou **8.5.13** (ou versions ultérieures). Redémarrer le service PHP-FPM après la mise à jour.

En l'absence d'application immédiate du correctif, désactiver la réutilisation des connexions backend :

- sous nginx : fastcgi_keep_conn off
- sous Apache mod_proxy_fcgi : enablereuse=off

Les configurations par défaut de nginx et Apache (sans réutilisation) ne sont pas exposées à l'attaque démontrée.

DOCUMENTATION :

Avis de sécurité PHP Group et références

- github.com/php/php-src/security/advisories/GHSA-qc49-hpvq-g2w6
- php.net/ChangeLog-8.php

CVE-2026-129289 :

- cve.org/CVERecord