INFO RÉSEAU · SÉCURITÉ NUMÉRIQUE · OCTOBRE 2026

Faille de sécurité PHP : le bon réflexe pour votre site internet

Une vérification rapide, à faire une fois, pour s'assurer que le site de votre établissement est bien à jour.

Pas d'inquiétude, mais pas d'oubli. Dans la plupart des cas, la correction est faite par votre hébergeur ou votre prestataire. L'essentiel est de **vérifier** que c'est bien le cas, et de le relancer si besoin.

EN BREF

QUOI ?

Deux failles critiques dans **PHP**, le langage qui fait tourner la majorité des sites web, rendues publiques le **21 octobre 2026** (alerte du CERT-FR).

QUI ?

Les sites sous **WordPress**, Joomla, Drupal, PrestaShop, Moodle… et les autres applications PHP hébergées sur le même serveur.

POURQUOI AGIR ?

Sur un serveur non mis à jour, une personne extérieure pourrait accéder aux **données du site** (familles, élèves, comptes…).

Versions de PHP protégées
ou toute version plus récente

8.2.35 **8.3.36** **8.4.27** **8.5.12**

VOTRE SITE EST HÉBERGÉ CHEZ UN PRESTATAIRE : 3 ÉTAPES

1 Je regarde ma version de PHP

Dans WordPress :

Outils › Santé du site › Infos › Serveur

Sinon : interface de l'hébergeur, rubrique « Hébergement », « Configuration » ou « PHP ».

2 Je compare

Ma version figure dans la liste ci-dessus (ou est plus récente) : **c'est bon**.

Elle est plus ancienne : le site est **à mettre à jour**. Si l'hébergeur le permet, passez à la version corrigée la plus récente compatible, après une sauvegarde complète.

3 Je contacte mon hébergeur

Même si tout semble à jour, demandez-lui :

- si PHP a été mis à jour, et à quelle date ;
- sinon, quand il le sera et quelle protection est en place d'ici là ;
- s'il a détecté une activité suspecte.

Vous hébergez vous-même votre site ?

Serveur dans vos locaux ou géré par votre équipe : la mise à jour vous revient. Le CERT-FR recommande :

1. **Isoler** le serveur (voire le mettre hors ligne) s'il est en version vulnérable ;
2. **Mettre à jour** PHP vers une version corrigée ;
3. **Remettre en ligne** une fois le bon fonctionnement vérifié.

Les versions antérieures à 8.2 ne recevront pas de correctif : une migration est nécessaire.

Un doute sur une intrusion ?

Signes à surveiller :

- pages modifiées ou inconnues ;
- comptes administrateurs que vous n'avez pas créés ;
- lenteurs inhabituelles, alerte de l'hébergeur ou d'un visiteur.

Coupez le site **Ne supprimez rien**

cybermalveillance.gouv.fr

Une question ? Rapprochez-vous de votre Udogec / Urogec, qui fera le lien avec la Fnogec si nécessaire.

Fnogec · Fédération nationale des organismes de gestion de l'enseignement catholique

Source : alerte CERT-FR · CVE-2026-109618 et CVE-2026-109619