

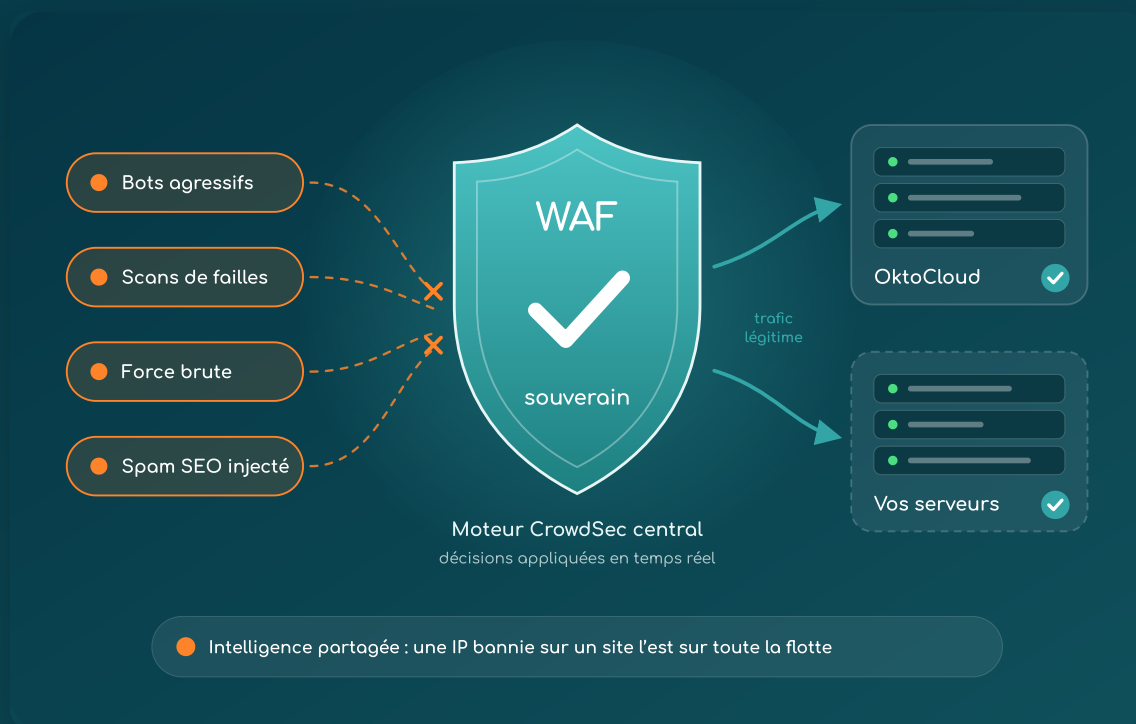


POST-MORTEM DE SÉCURITÉ

Faile PHP2Shell : retour sur une correction le jour même

Ce qui s'est passé, ce que nous avons fait et comment vos sites sont protégés, expliqué simplement.

CVE-2026-109618 · CVE-2026-109619 · gravité 9,2/10



INCIDENT CLOS

HÉBERGEMENT OKTOCLOUD

Faille critique PHP2Shell : vos sites ont été corrigés le jour même

Ce document explique ce qui s'est passé, ce que nous avons fait et quand, et comment votre hébergement est protégé. Il est rédigé pour être lisible sans connaissances techniques ; un glossaire figure en dernière page.

En bref

Le mardi 21 octobre 2026 à 16h, l'équipe qui développe PHP, le langage qui fait fonctionner vos sites WordPress, a publié le correctif de deux failles critiques. **Le soir même, l'ensemble des sites hébergés sur Oktocloud fonctionnaient sur une version corrigée de PHP**, et une protection supplémentaire avait été activée avant même la sortie du correctif.

16h00

Publication officielle du correctif (21/10)

17h48

Premier site en production sur PHP corrigé

23h01

Toutes les applications Oktocloud corrigées

192

Sites et applications vérifiés (26 + 166)

1. La faille, en deux mots

PHP est le « moteur » qui génère les pages de la plupart des sites web, dont tous les sites WordPress. Le 20 octobre, des informations ont fuité sur deux failles dans ce moteur, surnommées **PHP2Shell** (références officielles [CVE-2026-109618](#) et [CVE-2026-109619](#), gravité **9,2 sur 10**).

Concrètement, une simple requête envoyée par un attaquant pouvait lui permettre de **prendre le contrôle du serveur**, sans identifiant ni mot de passe. Toutes les versions de PHP depuis 2012 étaient concernées, et des tentatives d'attaque ont été observées dans le monde dès le matin du 21 octobre. L'équipe PHP a publié les versions corrigées le 21 octobre à 16h (heure de Paris).

2. Votre hébergement Oktocloud

Les sites que nous gérons sont hébergés sur l'une des deux plateformes d'Oktocloud, qui ont chacune été traitées selon leur fonctionnement :

Plateforme conteneurisée

26 sites et applications, chacun isolé dans son propre « conteneur ». **Nous maîtrisons entièrement la version de PHP** : nous avons construit nous-mêmes une version corrigée et l'avons déployée site par site.

Hébergement mutualisé

166 sites répartis sur 15 comptes, sur des serveurs **CloudLinux** exploités par notre hébergeur partenaire. Les mises à jour de PHP y sont installées par l'hébergeur ; **nous les avons vérifiées compte par compte**.

3. Chronologie des interventions

Toutes les heures sont exprimées en heure de Paris.

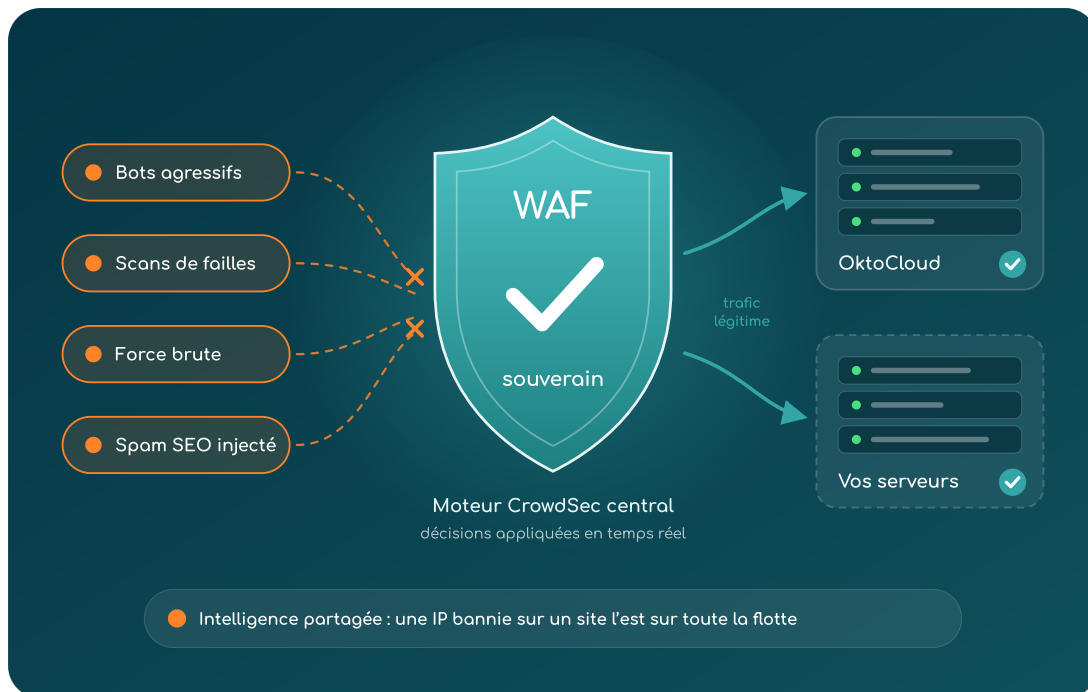
Date et heure	Événement / intervention
Lun. 20/10	Fuite des informations sur la faille. L'équipe PHP annonce un correctif pour le lendemain 16h. Analyse et préparation côté Oktocloud.
Mar. 21/10 · 15h59	Protection activée avant le correctif : le mécanisme de PHP visé par l'attaque (« suivi de progression des envois de fichiers ») est désactivé dans notre socle d'hébergement et déployé sur un premier site.
Mar. 21/10 · 16h00	Publication officielle des versions corrigées de PHP (8.2.35, 8.3.36, 8.4.27, 8.5.12).
Mar. 21/10 · 17h35	Nouvelle image d'hébergement PHP 8.4.27 construite par nos soins et validée par une série de tests automatiques (version servie, protection active, modules nécessaires à WordPress, cache).
Mar. 21/10 · 17h48	Premier site en production sur PHP 8.4.27 , moins de deux heures après la publication du correctif.
Mar. 21/10 · 17h57 → 23h01	Déploiement progressif sur les 26 sites et applications de la plateforme conteneurisée, par lots, avec contrôle de chaque site après mise à jour (page d'accueil, page de connexion, version de PHP).
Mar. 21/10 · 21h00	CloudLinux publie les versions corrigées de PHP pour ses serveurs (de PHP 5.2 à 8.5). Notre hébergeur mutualisé les installe sur ses serveurs.
Mer. 22/10 · nuit	Vérification des 15 comptes d'hébergement mutualisé (166 sites) : versions de PHP corrigées en place, et mécanisme visé également désactivé au niveau du serveur par l'hébergeur.
Mer. 22/10 · 00h58	Fin des opérations : toutes les plateformes sont à jour et homogènes.

4. Les protections en place sur Oktocloud

La correction de cette faille s'appuie sur plusieurs couches de sécurité, qui se complètent : si l'une est contournée, les autres restent actives.

① Un pare-feu applicatif (WAF) en frontal

Le trafic de la grande majorité des sites passe d'abord par notre **serveur frontal**, équipé du pare-feu collaboratif **CrowdSec**. Il détecte et bloque automatiquement les adresses qui sondent les sites à la recherche de failles, et s'appuie sur des listes d'attaquants partagées par des milliers de serveurs dans le monde. Il permet aussi d'appliquer en quelques minutes un « **patch virtuel** » sur tous les sites à la fois, lorsqu'une faille est connue mais pas encore corrigée.



② Des versions de PHP maîtrisées et mises à jour (plateforme conteneurisée)

Sur la plateforme conteneurisée, nous fabriquons nous-mêmes l'environnement PHP à partir des sources officielles, ce qui nous a permis de **passer en PHP 8.4.27 sans attendre les distributions tierces**. Chaque version est testée automatiquement avant d'être déployée, et l'ancienne reste disponible pour un retour arrière immédiat. L'ensemble des sites partage désormais un socle commun et à jour, ce qui accélère les prochaines mises à jour.

③ Des versions de PHP corrigées par CloudLinux (hébergement mutualisé)

Les serveurs d'hébergement mutualisé fonctionnent sous **CloudLinux**, qui a publié le soir du 21 octobre des versions de PHP intégrant le correctif, y compris pour les anciennes versions de PHP qui ne sont plus maintenues officiellement. CloudLinux applique le correctif sans changer le numéro de version affiché (par exemple « 8.4.26 » corrigé), selon sa pratique habituelle de « rétroportage ».

④ Une défense en profondeur

Le mécanisme de PHP utilisé par l'attaque **reste désactivé partout**, sur nos deux plateformes, même avec les versions corrigées. Aucun site WordPress n'en a besoin pour fonctionner. Si une variante de la faille apparaissait, elle trouverait la porte déjà fermée.

⑤ Un accès d'administration doublement sécurisé

L'accès à l'administration de vos sites est protégé par **Oktolink**, notre extension de sécurité : la page de connexion est masquée, et la connexion peut être renforcée au choix par une **double authentification classique** (un code temporaire généré par une application sur téléphone, en plus du mot de passe) ou par la **connexion unifiée Oktolink (SSO)**, qui centralise les accès et leur double authentification. **Ces protections sont activables sur simple demande.**

5. Impact

Les mises à jour ont été réalisées site par site, avec un contrôle systématique après chaque déploiement. Cette intervention avait pour objet de corriger la faille ; aucun incident de sécurité lié à PHP2Shell ne nous a été signalé sur les sites hébergés. Une analyse détaillée des journaux d'un site peut être réalisée sur demande.

6. Conclusion

Dès la déclaration de la faille, le correctif a été appliqué dans la foulée. Une première protection était en place avant même la publication officielle ; le premier site tournait sur la version corrigée moins de deux heures après sa sortie, et **l'ensemble des 192 sites et applications hébergés sur Oktocloud était corrigé et vérifié dans la nuit du 21 au 22 octobre.** Aucune action n'est requise de votre part.

Glossaire

PHP	Langage de programmation qui fait fonctionner la plupart des sites web, dont WordPress. Il s'exécute sur le serveur et fabrique les pages que voient vos visiteurs.
Faillle / CVE	Défaut de sécurité dans un logiciel. Chaque faille publique reçoit un identifiant unique « CVE » et une note de gravité sur 10.
Correctif (patch)	Nouvelle version d'un logiciel qui supprime la faille.
Patch virtuel	Règle de filtrage appliquée en amont des sites, qui bloque une attaque connue sans modifier les sites eux-mêmes, en attendant le correctif.
WAF (pare-feu applicatif)	Filtre placé devant les sites web, qui analyse le trafic et bloque les requêtes et les adresses malveillantes.
CrowdSec	Pare-feu collaboratif : les serveurs qui l'utilisent partagent les adresses des attaquants qu'ils détectent, ce qui permet de les bloquer partout.
Conteneur	Environnement isolé dans lequel fonctionne un site, avec sa propre version de PHP. Il peut être reconstruit et remplacé en quelques minutes.
CloudLinux	Système utilisé par de nombreux hébergeurs mutualisés, dont notre partenaire. Il fournit ses propres versions de PHP, maintenues et corrigées.
Rétroportage	Fait d'appliquer un correctif à une version existante d'un logiciel, sans changer son numéro de version.
Double authentification (2FA)	Connexion qui demande, en plus du mot de passe, un code temporaire généré par une application sur téléphone. Un mot de passe volé ne suffit plus.
SSO Oktolink	Connexion unifiée : un compte unique, protégé par double authentification, donne accès aux sites autorisés, au lieu d'un mot de passe par site.

Pour toute question sur ce document ou sur la sécurité de votre site, contactez votre interlocuteur habituel chez **Oktopod**.