Faille de sécurité critique dans une extension WordPress populaire : mettez à jour maintenant !

Actualités · https://kyzoe.be/fr/docs/faille-critique-extension-wordpress-populaire-mettez-a-jour/

Plus de 900 000 sites WordPress sont menacés par une faille grave dans l’extension WPvivid Backup & Migration. Votre site est-il lui aussi vulnérable ?

Que se passe-t-il ?

Des chercheurs en sécurité ont découvert une vulnérabilité dangereuse dans l’extension WPvivid Backup & Migration pour WordPress. Cette extension est utilisée par plus de 900 000 sites web dans le monde pour réaliser des sauvegardes et migrer des sites vers un autre environnement d’hébergement.

La vulnérabilité — officiellement connue sous le nom **CVE-2026-1357** — a reçu un score de gravité de **9,8 sur 10**. C’est pratiquement le maximum. Un attaquant sans le moindre accès à votre site web peut exploiter cette faille pour téléverser des fichiers malveillants et prendre ainsi le contrôle total de votre site.

Comment fonctionne exactement la faille ?

Pas besoin d’être un expert technique pour en comprendre l’essentiel : l’extension présente deux défauts à la fois.

Premièrement, un problème survient dans la manière dont l’extension chiffre les clés et les mots de passe. Si une étape de ce processus échoue, l’extension ne s’arrête pas — elle continue simplement avec une "fausse clé" prévisible. Un attaquant qui le sait peut en profiter pour envoyer de faux fichiers que l’extension considère comme légitimes.

Deuxièmement, l’extension ne vérifie pas correctement les noms des fichiers téléversés. Un attaquant peut ainsi placer des fichiers en dehors du dossier protégé — y compris des fichiers PHP malveillants permettant de prendre le contrôle du site de l’intérieur.

Êtes-vous vulnérable ?

Tous les utilisateurs de l'extension ne courent pas le même risque. Vous êtes **uniquement vulnérable de manière critique** si vous avez activé l'option "*recevoir une sauvegarde d'un autre site web*". Elle est désactivée par défaut, mais de nombreux gestionnaires de sites l'activent lorsqu'ils migrent un site d'un environnement d'hébergement à un autre.

De plus, un attaquant ne dispose que d'une fenêtre de 24 heures pour exploiter la faille, car la clé nécessaire à l'attaque expire après un jour. Ce n'est toutefois pas une raison pour baisser la garde : si vous utilisez régulièrement l'extension pour des migrations, cette fenêtre s'ouvre à plusieurs reprises.

Que devez-vous faire ?

Le conseil est clair : **mettez immédiatement à jour l'extension WPvivid vers la version 0.9.124 ou supérieure.**

Cette mise à jour a été publiée le 28 janvier et apporte trois améliorations concrètes :

- L'extension s'arrête désormais correctement lorsque le chiffrement échoue, au lieu de continuer avec une clé non sécurisée.
- Les noms de fichiers sont désormais correctement vérifiés, de sorte que les attaquants ne peuvent plus placer de fichiers en dehors du dossier sécurisé.
- Seuls les types de fichiers autorisés sont encore acceptés (comme ZIP, GZ, TAR et SQL).

La chronologie en bref

Date	Que s'est-il passé ?
12 janvier	Le chercheur Lucas Montes (NiRoX) découvre la faille et la signale
22 janvier	La société de sécurité Defiant informe le développeur WPVividPlugins
28 janvier	La version 0.9.124 contenant le correctif est publiée

Conclusion

Il s'agit d'une vulnérabilité sérieuse que vous ne devez pas ignorer. Le risque d'exploitation est réel, surtout si vous utilisez l'extension pour des migrations de sites. Vérifiez dès aujourd'hui quelle version de WPvivid vous utilisez et mettez-la à jour si nécessaire.

Vous avez besoin d’aide pour sécuriser votre site WordPress ou vous souhaitez savoir si votre site est vulnérable ? **Contactez Kyzoe** — nous vous aiderons avec plaisir.

Source : Defiant / Wordfence Security Research