Une faille zero day réinitialise l'admin de WordPress

Le chercheur en sécurité Dawid Golunski a relevé une vulnérabilité zero day (CVE-2017-8295) dans WordPress (versions 4.7.4 et précédentes). *« Wordpress dispose d'une fonction de réinitialisation de mot de passe victime d'une vulnérabilité qui pourrait, dans certains cas, permettre aux attaquants d'obtenir le lien de réinitialisation du mot de passe sans authentification antérieure*, prévient l'expert dans son alerte. *Une telle attaque pourrait amener un attaquant à obtenir un accès non autorisé au compte WordPress d'une victime. »* Autrement dit, prendre la main sur l'administration du site opéré par la plate-forme de gestion de contenus (CMS). Un sérieux problème pour la solution utilisée par 60 millions de sites dont plus de 27% des 10 millions les plus populaires.

Récupérer l'e-mail de réinitialisation

Le problème vient de la conception du logiciel qui s'appuie sur des données non approuvées par défaut lors de l'envoi d'un e-mail de réinitialisation du mot de passe quand celui-ci a été oublié par son détenteur. L'e-mail de réinitialisation qui doit arriver dans la boîte de son supposé demandeur, pourrait être détourné, ou plutôt récupéré, par un attaquant. Dawid Golunski le constate dans le code de la plate-forme. Grossièrement, la faille tient dans la possibilité de modifier la variable SERVER_NAME pour ajouter un entête d'expéditeur (From/Return-Path) dans le courriel de réinitialisation. Par exemple, le domaine 'attackers-mxserver.com' pour générer l'adresse 'wordpress@attackers-mxserver.com' dans la variable $from_email.

Cette modification peut, selon la configuration du serveur de messagerie, générer un courrier électronique envoyé à l'utilisateur victime de WordPress avec l'adresse malveillante définie dans les en-têtes du message. *« Cela pourrait permettre à l'attaquant d'intercepter le courrier électronique contenant le lien de réinitialisation du mot de passe nécessitant, ou pas selon les cas, une interaction de l'utilisateur »*, explique le chercheur.

Trois méthode de récupération

Reste à savoir comment intercepter le courriel en question. Dawid Golunski avance trois possibilités : dans la première, l'attaquant lance une attaque DoS sur le compte e-mail de sa victime afin que le message de réinitialisation n'atteigne pas la boîte de son propriétaire légitime et soit renvoyé vers l'adresse de l'attaquant; dans la deuxième, certains systèmes de réponse pourraient joindre une copie du message de réinitialisation vers l'e-mail de l'attaquant; enfin, dans la troisième, la victime pourrait répondre directement à cet e-mail de réinitialisation (pour, par exemple, s'étonner de recevoir un tel message de réinitialisation). Réponse qui tomberait dans la boîte de l'attaquant avec le lien de réinitialisation.

Pour l'heure, WordPress n'a publié aucun correctif à cette vulnérabilité alors que ses développeur et la communauté du CMS Open Source en a été alertés en juillet 2016. *« Puisque cette affaire n'a pas progressé depuis, cette vulnérabilité est finalement rendue publique sans un correctif officiel »*, annonce sans

sourciller Dawid Golunski qui a, il est vrai, fait preuve de patience. En attendant le patch, il propose une alternative : celle d'utiliser une valeur SERVER_NAME statique. Comme l'explique la directive UseCanonicalName disponible sur cette page. Reste que les administrateurs de sites sous WordPress doivent désormais redoubler de vigilance.

Lire également
OVH et Iliad hébergent de nombreuses attaques contre WordPress
Une faille dans PHPMailer fragilise des CMS et des millions de sites web
Une faille zero day sur les serveurs Apache massivement exploitée

Crédit Photo: Evan Lorne-Shutterstock