AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Une porte dérobée dormante dans un plugin WordPress

Contenu

I. Contexte

Une vulnérabilité majeure, de type porte dérobée (backdoor), a été découverte par les chercheurs dans l'extension WordPress populaire **Quick Page/Post Redirect.** Initialement conçue pour gérer des redirections d'URLs, cette extension a été compromise il y a environ cinq ans, permettant l'injection de code arbitraire sur plus de 70 000 sites web.

II. Analyse de l'incident et découverte

L'alerte a été donnée par l'hébergeur Anchor, après que douze sites de son infrastructure ont déclenché des alertes de sécurité. Les recherches ont révélé que le malware est resté tapi dans l'ombre pendant plusieurs années sans être détecté.

Bien que l'extension soit un outil utilitaire standard, les versions publiées entre 2020 et 2021 ont servi de vecteur d'attaque sophistiqué.

Mécanisme de compromission : Le "Self-Updater" malveillant

Les versions officielles **5.2.1 et 5.2.2** incluaient un mécanisme de mise à jour dissimulé pointant vers un domaine tiers : www.anadnet.com. Ce système permettait de pousser du code arbitraire en dehors du contrôle et de la surveillance du dépôt officiel WordPress.org.

En mars 2021, les sites utilisant ces versions ont reçu silencieusement une version 5.2.3 infectée provenant de ce serveur externe. Cette version contenait une porte dérobée passive, dont l'empreinte numérique (hash) différait totalement de la version légitime disponible sur WordPress.org à l'époque.

Une fois cette infrastructure de contrôle en place, les attaquants ont pu exploiter les sites à des fins lucratives tout en restant invisibles.

III. Objectif de l'attaque

Spam SEO et Persistance

La porte dérobée a été conçue pour être particulièrement discrète, elle ne s'active que pour les utilisateurs non connectés, afin de cacher son activité aux administrateurs du site. Techniquement, elle se greffe sur le *hook the_content* pour récupérer des données depuis le serveur malveillant.

Selon les chercheurs, il s'agissait d'une opération de "SEO parasite". L'objectif était de détourner le référencement Google de 70 000 sites au profit d'opérateurs tiers. Cependant, le danger réel réside dans le mécanisme de mise à jour lui-même, qui permet d'exécuter n'importe quel code à la demande. Bien que le sous-domaine de commande et contrôle (C2) soit actuellement inactif, le domaine principal reste actif, représentant une menace latente permanente.

Face à ce risque de reprise d'activité malveillante, des mesures immédiates sont nécessaires pour sécuriser les sites WordPress.

IV. Conclusion

À l'heure actuelle, WordPress.org a temporairement retiré l'extension de son répertoire officiel en attendant un examen approfondi. Néanmoins des actions urgentes sont requises à savoir :

- Désinstallation immédiate de l'extension du tableau de bord WordPress ;
- Réinstaller une version saine (5.2.4 ou supérieure) provenant exclusivement du dépôt officiel WordPress.org ;
- Inspecter les fichiers pour détecter toute trace de communications sortantes vers le domaine www.anadnet.com.