« The most common cybercrime is no crime at all. It's just a failure to secure the system.»
- Kevin Mitnick -

BULLETIN DE VEILLE N°11

ANPT-2024-BV-11

Novembre 2024

Alertes de sécurité

Wordpress

CVE-2024-10542 & CVE-2024-10781 : Une faille critique dans un plugin WordPress expose 200 000 sites

25 Novembre 2024

Un récent rapport de l'équipe de veille sur les menaces de Wordfence a révélé deux vulnérabilités critiques dans le plugin WordPress Anti-Spam by CleanTalk, affectant plus de 200 000 installations actives. Ces vulnérabilités, identifiées comme CVE-2024-10542 et CVE-2024-10781, pourraient permettre à des attaquants non authentifiés de compromettre des sites web en installant des plugins malveillants et en exécutant du code arbitraire, l'usurpation de DNS inversé et les vérifications de clés API vides conduisent à un contournement de l'autorisation.

La première vulnérabilité, CVE-2024-10542, provient d'un problème de contournement d'autorisation lié à l'usurpation de DNS inverse. Comme l'explique le rapport, « l'adresse IP est déterminée sur la base des paramètres d'en-tête X-Client-Ip et X-Forwarded-By, qui sont des paramètres définis par l'utilisateur, ce qui rend cette fonction vulnérable à l'usurpation d'adresse IP ». Cette faille permet aux attaquants de manipuler les enregistrements DNS et de contourner les contrôles d'authentification, ce qui leur donne la possibilité d'installer et d'activer des plugins à distance. Cette faille a été divulguée de manière responsable par le chercheur mikemyers dans le cadre du programme Wordfence Bug Bounty, ce qui lui a valu une prime de 4 095,00 $.

La seconde vulnérabilité, CVE-2024-10781, provient d'une vérification manquante de la valeur vide de la clé API. « Malheureusement, la fonction n'inclut aucune vérification pour empêcher l'autorisation lorsque la clé API est vide », indique le rapport. Cela signifie que les sites dont la clé API n'est pas configurée sont vulnérables à un accès non autorisé, ce qui permet aux attaquants d'effectuer des actions telles que l'installation et l'activation de plugins.

Les deux vulnérabilités ont un score CVSS de 9,8, ce qui souligne leur gravité et leur potentiel d'exploitation à grande échelle. L'équipe de veille sur les menaces de Wordfence recommande vivement à tous les utilisateurs du plugin Anti-Spam by CleanTalk de mettre à jour immédiatement leur site avec la dernière version corrigée, la 6.45.

« Nous recommandons vivement aux utilisateurs de mettre à jour leurs sites avec la dernière version corrigée d'Anti-Spam by CleanTalk, la version 6.45 à l'heure où nous écrivons ces lignes, dès que possible », souligne le rapport.

Source : https://bit.ly/3xO9sQF

PHP

PHP corrige plusieurs failles, dont CVE-2024-8932 (CVSS 9.8)

27 Novembre 2024

L'équipe de développement de PHP a publié des mises à jour de sécurité urgentes pour corriger plusieurs vulnérabilités affectant les versions antérieures à 8.1.31, 8.2.26, et 8.3.14. Ces vulnérabilités sont plus ou moins graves, certaines pouvant permettre à des attaquants de divulguer des informations sensibles, d'exécuter du code arbitraire ou de lancer des attaques par déni de service.

L'une des vulnérabilités les plus graves, CVE-2024-8932, permet un accès hors limites (OOB) dans la fonction ldap_escape. Cette vulnérabilité, avec un score CVSS de 9.8, pourrait permettre à des attaquants d'exécuter un code arbitraire sur les systèmes affectés.

« Les entrées de chaînes longues non contrôlées dans ldap_escape sur les systèmes 32 bits peuvent provoquer un débordement d'entier, entraînant une écriture hors limites », prévient l'avis.

Une autre faille critique, CVE-2024-8929, permet aux attaquants de faire fuir le contenu partiel du tas par le biais d'une lecture excessive de la mémoire tampon du tas. Cette vulnérabilité peut être exploitée en se connectant à un faux serveur MySQL ou en manipulant des paquets réseau. « En utilisant PHP-FPM qui reste en vie entre les requêtes, et entre deux requêtes SQL différentes, il est possible d'extraire le contenu de la réponse de la requête MySQL précédente à partir du travailleur PHP-FPM », explique l'avis. Une démonstration de faisabilité a montré comment un faux serveur MySQL pouvait manipuler les en-têtes des paquets pour extraire les données résiduelles de la mémoire tampon.

En plus de ces vulnérabilités critiques, la mise à jour corrige également plusieurs autres problèmes, notamment : CVE-2024-11233 CVE-2024-11234 CVE-2024-11236

Source : https://bit.ly/3xO9sQF

Actualité

Une cyberattaque présumée en faveur de l'Ukraine met hors service les services de stationnement d'une ville russe

Les habitants de la ville de Tver, dans le nord-ouest de la Russie, ont pu se garer gratuitement pendant près de deux jours en raison de ce que les autorités locales ont appelé une « défaillance technique » du système de paiement numérique du stationnement.

Toutefois, un groupe de pirates informatiques connu sous le nom d'Ukrainian Cyber Alliance avance une autre raison possible à cette perturbation : une cyberattaque sur le réseau administratif de la ville.

Dans un communiqué publié mardi, le porte-parole du groupe a déclaré que les pirates avaient mis le réseau hors service et qu'ils avaient effacé « des dizaines de machines virtuelles, le stockage de sauvegarde, les sites web, le courrier électronique et des centaines de postes de travail ».

« Ils n'ont plus rien. L'internet est coupé, les téléphones ne fonctionnent plus, et même le système de parking est mort », a affirmé le porte-parole, en partageant des captures d'écran des systèmes prétendument violés pour étayer ses affirmations.

Dans un premier temps, les autorités de Tver n'ont pas commenté la revendication des pirates, bien que certains experts locaux en cybersécurité aient noté que le site web officiel de la ville était hors ligne. Un jour après l'attaque présumée, l'administration de Tver a publié une déclaration indiquant que des travaux techniques étaient en cours sur son site web et sur la plateforme de paiement en ligne du stationnement, ce qui les rendait temporairement indisponibles.

Les résidents locaux ont signalé que lorsqu'ils tentaient d'effectuer un paiement, ils recevaient des messages d'erreur ou subissaient des échecs de chargement de l'application, avec une erreur de « délai d'attente ».

Jeudi, les autorités municipales ont annoncé que les services de paiement du stationnement avaient été rétablis, sans toutefois confirmer s'il s'agissait d'une cyberattaque.

Ce n'est pas la première fois que des pirates pro-Ukraine revendiquent des attaques contre des services russes. Au début du mois d'octobre, des pirates de l'équipe BO, un groupe pro-Ukraine connu pour avoir coopéré avec les services de renseignement militaire ukrainiens dans le cadre de plusieurs opérations contre la Russie, ont déclaré avoir pénétré dans le système utilisé par les tribunaux russes.

À la suite de cette attaque, les sites web des tribunaux russes de droit commun sont restés inaccessibles pendant des semaines, de même que leur réseau de communication et leurs services de courrier électronique. À l'époque, les pannes des sites web des tribunaux ont également été attribuées à une « défaillance technique ».

Source : https://bit.ly/3WklED7

Le géant des jeux d'argent et des loteries, perturbé par une cyberattaque

L'une des plus grandes sociétés de jeux d'argent des États-Unis a déclaré qu'une cyberattaque survenue la semaine dernière avait provoqué des perturbations massives dans ses activités, l'obligeant à mettre certains systèmes hors ligne.

L'International Game Technology (IGT) a informé mardi la Securities and Exchange Commission des États-Unis qu'elle avait eu connaissance de la cyberattaque lorsqu'elle avait « connu des perturbations dans certaines parties de ses systèmes et applications informatiques internes » le dimanche.

« La société a également mis hors ligne certains systèmes de manière proactive afin de les protéger. L'enquête en cours et la réponse de la société comprennent des efforts pour remettre ses systèmes en ligne », a déclaré la société.

La société a ajouté qu'elle n'avait pas encore déterminé si cela aurait un impact sur ses résultats, et qu'elle avait mis en place des solutions de contournement pour continuer à servir ses clients.

IGT fournit des systèmes et des technologies pour les loteries, les machines à sous et les paris sportifs. La société emploie plus de 11 000 personnes dans le monde et a déclaré un chiffre d'affaires de 1,9 milliard de dollars pour les neuf premiers mois de l'année.

Aucun groupe de pirates informatiques n'a revendiqué l'attaque jusqu'à jeudi, mais des opérations de ransomware ont ciblé à plusieurs reprises des casinos et des loteries au cours de l'année écoulée.

La loterie de l'État de l'Ohio a été touchée par un ransomware l'année dernière et la perturbation du casino MGM à l'automne dernier a causé plus de 100 millions de dollars de dommages. Hier, le ministère de la justice a rendu publiques les accusations portées contre plusieurs des pirates informatiques impliqués dans l'incident.

Source : ***https://bit.ly/3w81ktP***

Bon à savoir

Evité tous les sites non sécurisés

Les sites de confiance sont des sites web qui prennent les mesures nécessaires pour sécuriser vos données et protéger votre vie privée. Ces sites utilisent généralement HTTPS (HyperText Transfer Protocol Secure), qui chiffre les données pendant leur transmission, rendant beaucoup plus difficile pour les pirates d'intercepter ou de manipuler vos informations. Les sites de confiance possèdent également des certificats de sécurité mis à jour et adoptent des pratiques telles que l'authentification à deux facteurs et des audits de sécurité réguliers. Vous pouvez facilement détecter un site de confiance en recherchant l'icône de cadenas dans la barre d'adresse du navigateur et en vous assurant que l'URL commence par "https://". De plus, un site de confiance affiche souvent des certificats de sécurité lorsque vous cliquez sur le cadenas, confirmant ainsi la légitimité du site.

En revanche, les sites non sécurisés sont ceux qui manquent de chiffrement HTTPS ou qui possèdent des certificats de sécurité obsolètes ou invalides. Ces sites mettent vos informations personnelles en danger car toutes les données échangées sur une connexion HTTP sont non chiffrées et peuvent être interceptées par des cybercriminels. Les sites non sécurisés commencent souvent par "http://" et peuvent afficher des messages d'avertissement dans le navigateur, tels que "Non sécurisé", pour signaler l'absence de chiffrement. Pour vous protéger, évitez d'entrer des informations sensibles, telles que des mots de passe ou des informations de paiement, sur des sites non sécurisés, et vérifiez toujours les caractéristiques de sécurité d'un site avant de procéder à des transactions.

Visiter un site non sécurisé peut vous exposer à divers risques, tels que le vol de données, les infections par des logiciels malveillants et le vol d'identité. Étant donné que ces sites manquent souvent de chiffrement ou ont une sécurité compromise, les cybercriminels peuvent facilement intercepter vos informations personnelles, telles que des mots de passe ou des numéros de carte bancaire. De plus, les sites non sécurisés peuvent héberger des logiciels malveillants qui peuvent infecter votre appareil, entraînant des pertes de données ou des violations de sécurité supplémentaires. Dans certains cas, des attaquants peuvent utiliser ces sites pour du phishing, vous incitant à révéler des informations sensibles. Il est donc crucial d'éviter d'interagir avec des sites non sécurisés pour protéger votre vie privée et votre sécurité en ligne.

Evènements

Evènement à venir

SECURA Afrique du Nord - Expo & Conférence 2024

03 - 05 Déc. 2024

Safex - Foire d'Alger, Mohammadia, Algérie

https://bit.ly/4d9tYeF

C'est le 6ème salon international de la sureté, de la sécurité, du feu et de l'urgence en Afrique du Nord**,** SECURA rassemble au même endroit pendant 3 jours tous les acteurs et professionnels du domaine de la sécurité industrielle, commerciale et intérieure, de la sécurité du travail, de la lutte contre les incendies, de la cybersécurité et de l'urgence.

Laissez-vous inspirer par plus de 20 conférenciers couvrant de multiples sujets tels que : la lutte contre les incendies, la cybersécurité, la sécurité au travail, les urgences et bien plus encore.

Référence	ANPT-2024-BV-11
Titre	Bulletin de veille N°11
Date de version	30 Novembre 2024
Contact	ssi@anpt.dz