BULLETIN DE VEILLE N°01

ANPT-2024-BV-01

« One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. »
- Stephane Nappo -

Janvier 2024

Alertes de sécurité

Apple

Apple corrige une faille critique dans les iPhones et les Macs

23 Janvier 2024

Apple a publié lundi des mises à jour de sécurité pour iOS, iPadOS, macOS, tvOS et le navigateur web Safari afin de corriger une vulnérabilité zero-day activement exploitée dans la nature. Repérée comme CVE-2024-23222, la faille est un bogue de confusion de type dans le moteur de navigation WebKit, permettant aux acteurs de la menace d'exécuter du code arbitraire lors du traitement de contenus web malveillants.

Les failles de type confusion, comme celle-ci, peuvent entraîner des accès hors limites à la mémoire, des plantages et l'exécution de code arbitraire. Bien qu'Apple ait reconnu être au courant de l'exploitation du problème, elle n'a fourni aucun détail sur la nature des attaques ou les acteurs impliqués.

Les mises à jour sont disponibles pour divers appareils et systèmes d'exploitation, notamment iOS 17.3, iPadOS 17.3, iOS 16.7.5, iPadOS 16.7.5, macOS Sonoma 14.3, macOS Ventura 13.6.4, macOS Monterey 12.7.3, tvOS 17.3 et Safari 17.3.

Il s'agit du premier correctif d'Apple pour une vulnérabilité zero-day activement exploitée au cours de l'année 2024, après que l'entreprise a corrigé 20 vulnérabilités de ce type dans le cadre d'attaques réelles au cours de l'année précédente.

En outre, Apple a rétroporté les correctifs pour CVE-2023-42916 et CVE-2023-42917, initialement publiés 2023, sur les anciens appareils fonctionnant sous iOS 15.8.1 et iPadOS 15.8.1.

Source : *https://bit.ly/3w10Bu8*

Kyocera

Les imprimantes Kyocera sont vulnérables au détournement de chemin d'accès

09 Janvier 2024

Une équipe de chercheurs a découvert une vulnérabilité de traversée de chemin dans le produit Device Manager de Kyocera, conçu pour superviser de vastes parcs d'imprimantes dans les moyennes et grandes entreprises.

Selon la filiale américaine de la division d'imagerie bureautique de Kyocera, l'exploitation de cette vulnérabilité nécessite qu'un attaquant soit connecté au réseau pour l'exploiter et constituer une véritable menace.

Trustwave, une société de cybersécurité, a initialement divulgué cette faille dans un billet de blog. Kyocera a rapidement publié un correctif pour remédier à la vulnérabilité.

La vulnérabilité identifiée, CVE-2023-50916, implique une attaque par traversée de chemin. Les attaquants peuvent manipuler le chemin local de la base de données de sauvegarde, ce qui incite le logiciel de gestion d'impression à valider l'accès et à authentifier le chemin.

Trustwave a noté que Kyocera avait mis en place une protection : « l'interface graphique du logiciel rejette les tentatives de redéfinition du chemin d'accès à la base de données de sauvegarde si la nouvelle adresse contient une barre oblique », indiquant qu'elle pointe vers une ressource en réseau suivant la norme de la convention de nommage universelle. Cependant, les chercheurs ont trouvé un moyen de contourner cette restriction en utilisant un proxy d'interception web ou en envoyant directement la demande de nouveau chemin au point de terminaison de l'application.

Lors de l'établissement du nouveau chemin vers une ressource réseau contrôlée par l'attaquant, le logiciel de Kyocera authentifie le chemin. Trustwave a souligné que le message d'authentification, qui contient des identifiants Active Directory hachés, varie en fonction de l'environnement informatique. Si les administrateurs Windows n'ont pas activé la politique, les hachages NTLM peuvent être inclus dans le message d'authentification.

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

Actualité

Des attaquants visent un plugin WordPress de base de données actif sur 1 million de sites

Des chercheurs ont détecté une activité malveillante ciblant une vulnérabilité de gravité critique dans le plugin WordPress "Better Search Replace". Ce plugin, largement utilisé avec plus d'un million d'installations, facilite les opérations de recherche et de remplacement dans les bases de données lors de la migration de sites web vers de nouveaux domaines ou serveurs.

Le fournisseur du plugin, WP Engine, a publié la version 1.4.5 pour corriger une vulnérabilité d'injection d'objet PHP de gravité critique identifiée sous le nom de CVE-2023-6933. Cette vulnérabilité provient de la désérialisation d'entrées non fiables, ce qui permet à des attaquants non authentifiés d'injecter un objet PHP. Une exploitation réussie peut entraîner l'exécution de code, l'accès non autorisé à des données sensibles, la manipulation ou la suppression de fichiers, et le déclenchement d'un déni de service par boucle infinie.

Bien que Better Search Replace ne soit pas directement vulnérable, il peut être exploité pour exécuter du code, récupérer des données sensibles ou supprimer des fichiers si un autre plugin ou thème sur le même site contient la chaîne de programmation orientée propriété (POP). L'exploitabilité des vulnérabilités d'injection d'objets en PHP dépend souvent de la présence d'une chaîne POP appropriée qui peut être déclenchée par l'objet injecté pour effectuer des actions malveillantes.

L'entreprise de sécurité Wordfence a déclaré avoir bloqué plus de 2 500 attaques ciblant CVE-2023-6933 sur ses clients au cours des dernières 24 heures. La vulnérabilité affecte toutes les versions de Better Search Replace jusqu'à la version 1.4.4, et il est vivement conseillé aux utilisateurs de passer rapidement à la version 1.4.5.

Wordfence a notamment précisé que sa règle de détection initiale couvrait diverses activités, dont certaines liées à d'autres vulnérabilités telles que CVE-2023-25135. Toutefois, la majorité des attaques étaient liées à des tentatives d'exploitation de la vulnérabilité CVE-2023-6933. Les statistiques de téléchargement sur WordPress.org indiquent près d'un demi-million de téléchargements du plugin au cours de la semaine écoulée, 81 % des versions actives étant des versions 1.4, bien que la version mineure n'ait pas été précisée.

Source : *https://bit.ly/3Uki0b5*

26 milliards d'enregistrements divulgués pouvant être utilisés pour des attaques plus sérieuses

Une violation de données énorme, appelée la "Mère de toutes les violations" (MOAB), a été découverte. Elle comprend 12 téraoctets d'informations, soit plus de 26 milliards d'enregistrements. Cette fuite massive comprend des données provenant de brèches antérieures affectant des plateformes telles que LinkedIn, Twitter, Weibo, Tencent et d'autres, ce qui en fait sans doute la plus importante jamais découverte.

Le chercheur en sécurité Bob Dyachenko et l'équipe de Cybernews ont identifié des milliards d'enregistrements exposés sur une instance ouverte. Alors que le propriétaire de la base de données était initialement inconnu, Leak-Lookup, un moteur de recherche sur les violations de données, en a revendiqué la propriété, attribuant la fuite à une "mauvaise configuration du pare-feu" qui a depuis été corrigée.

Le MOAB comprend plus de 26 milliards d'enregistrements répartis dans 3 800 dossiers, chacun correspondant à une violation de données distincte. Bien qu'une grande partie des données divulguées proviennent de violations antérieures, il est probable qu'elles contiennent des informations inédites. Le propriétaire de l'ensemble de données est soupçonné d'être un acteur malveillant, un courtier en données ou un service traitant d'importants volumes de données.

Cette compilation massive constitue une menace sérieuse, les acteurs de la menace pouvant l'utiliser pour l'usurpation d'identité, l'hameçonnage sophistiqué, les cyberattaques ciblées et l'accès non autorisé à des comptes personnels. Bien que l'ensemble de données ne soit pas entièrement nouveau, son ampleur et la variété des informations sensibles qu'il contient dépassent les compilations précédentes, telles que la Compilation of Many Breaches (COMB) signalée en 2021.

L'impact potentiel sur les utilisateurs est considérable, car ces données massives augmentent le risque d'attaques de type "credential-stuffing" en raison de la pratique courante de réutilisation des mots de passe par les utilisateurs. Il est recommandé aux utilisateurs d'utiliser des mots de passe forts et uniques, d'activer l'authentification multifactorielle, de rester vigilants face aux tentatives d'hameçonnage, de vérifier les doublons de mots de passe et de sécuriser rapidement les comptes partageant les mêmes mots de passe. Un outil de vérification des fuites de données est en cours de mise à jour afin d'aider les utilisateurs à déterminer si leurs données font partie de cette faille majeure.

Source : *https://bit.ly/3HNM2MR*

Bon à savoir

Les mots de passe plus longs ne sont pas protégés contre les tentatives intensives de piratage

Un rapport récent de KrakenLab a mis en évidence diverses failles de sécurité liées aux mots de passe, en soulignant que les mots de passe longs ne sont pas à l'abri des violations. Les résultats révèlent que 31,1 millions de mots de passe violés comportaient plus

de 16 caractères, ce qui remet en question l'hypothèse selon laquelle la longueur seule garantit la sécurité des mots de passe. En outre, le rapport a identifié 40 000 comptes de portail d'administration utilisant "admin" comme mot de passe, et seulement 50 % des organisations recherchent les mots de passe compromis plus d'une fois par mois.

Le mot de passe le plus souvent compromis est "123456", ce qui reflète la prévalence des mots de passe faibles. Des mots de passe simples comme "Pass@123" et "P@ssw0rd", qui répondent aux règles de base de l'Active Directory, étaient également très répandus, soulignant le risque accru de réutilisation des mots de passe dans les organisations dépourvues de contrôles stricts des mots de passe.

Les cybercriminels continuent d'exploiter les mots de passe faibles au moyen de diverses techniques, notamment les attaques par dictionnaire, les attaques par force brute et les attaques par masque. Les attaques par dictionnaire consistent à deviner les mots de passe à l'aide de listes prédéfinies de possibilités probables, tandis que les attaques par force brute tentent toutes les combinaisons de caractères possibles. Les attaques par masque, une forme de force brute, ciblent des éléments connus de constructions de mots de passe courantes, réduisant ainsi le nombre de suppositions nécessaires.

Le rapport met l'accent sur la menace que représentent les "keyboard walks", où les caractères sont adjacents sur un clavier. Bien qu'apparemment aléatoires, ces motifs, tels que "Qwerty", sont fréquemment utilisés et ciblés par les pirates dans les attaques par dictionnaire et par force brute.

Il est essentiel de protéger tous les comptes, en particulier les comptes d'administrateur, car la compromission d'un compte d'administrateur permet d'obtenir un accès important sans qu'il soit nécessaire de procéder à une escalade des privilèges. Les utilisateurs privilégiés étant des cibles de choix, il est essentiel de mettre en place des mots de passe forts et uniques et d'appliquer des politiques de mot de passe pour atténuer les risques de cybersécurité. Malgré les améliorations apportées aux politiques en matière de mots de passe, le rapport souligne que les mots de passe restent un point faible important dans les stratégies de cybersécurité de nombreuses organisations.

Source : *https://bit.ly/49iTICA*

Evènements

Evènement à venir

Cyber Risk Series - Cloud Security Edition

28 Février 2024

En ligne

https://bit.ly/3SkyM7t

La sécurité du cloud est un terrain complexe, avec des défis spécifiques qui exigent une attention particulière. Un grand nombre d'équipes n'ont pas une connaissance approfondie des stratégies les plus efficaces dans l'environnement cloud contemporain.

Cette conférence est l'occasion d'obtenir des informations auprès d'experts du secteur qui vous fourniront des conseils précieux. Découvrir ce que les responsables de la sécurité doivent savoir pour protéger leurs actifs dans le cloud contre les menaces croissantes de ses jours.

Référence	ANPT-2024-BV-01
Titre	Bulletin de veille N°01
Date de version	31 Janvier 2024
Contact	ssi@anpt.dz