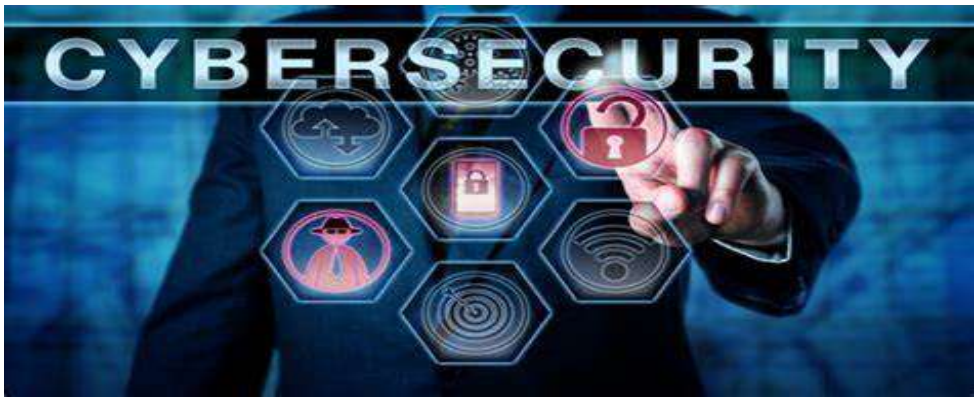

BULLETIN DE VEILLE N°03

ANPT-2023-BV-03

"Cybersecurity is a subject that requires logic, knowledge, thought and commitment."
— Ian R. McAndrew, PhD--

Mars 2023

Alertes de sécurité

Chrome

La mise à jour de Chrome 111 corrige des vulnérabilités de haute gravité

22 Mars 2023

Google a annoncé une mise à jour de Chrome 111 qui apporte des correctifs pour huit vulnérabilités.
Sept de ces problèmes sont des bogues de sécurité de la mémoire de haute sévérité, quatre d'entre eux étant décrits comme des vulnérabilités de type "use-after-free", un type de bogue pouvant entraîner l'exécution de code arbitraire, la corruption de données ou un déni de service.
La plus importante de ces vulnérabilités est la CVE-2023-1528, une faille de type "use-after-free" dans le composant "Passwords" de Chrome.
Vient ensuite la CVE-2023-1529, un accès à la mémoire hors limites dans WebHID.
Trois autres problèmes liés à l'utilisation après la fermeture ont été résolus dans le format PDF, dans le moteur graphique ANGLE et dans WebProtect.
La dernière mise à jour de Chrome 111 apporte également des correctifs pour deux problèmes de lecture hors limites dans GPU Video et ANGLE, elles ont été signalées par des chercheurs en sécurité du Google Project Zero.
Le géant de l'internet n'a fait aucune mention de l'exploitation de ces vulnérabilités dans des attaques.
La dernière version de Chrome est maintenant disponible en tant que version 111.0.5563.110 pour Mac et Linux et en tant que versions 111.0.5563.110/.111 pour Windows.

Source : https://bit.ly/3zaL2Oy

Microsoft

Microsoft propose des mises à jour de sécurité OOB pour la faille de l'outil Windows Snipping

24 Mars 2023

Microsoft a publié une mise à jour de sécurité d'urgence OOB pour l'outil Snipping de Windows 10 et Windows 11 afin de corriger la vulnérabilité de confidentialité Acropalypse.

Désormais répertoriée sous le nom de CVE-2023-28303, la vulnérabilité Acropalypse est due au fait que les éditeurs d'images ne suppriment pas correctement les données de l'image recadrée lorsqu'ils écrasent le fichier d'origine. Des données supplémentaires sont enregistrées après le marqueur de fichier IEND, qui indique la fin d'un fichier PNG. Normalement, il ne devrait pas y avoir de données après le marqueur IEND.

Ces données supplémentaires pourraient être utilisées pour récupérer partiellement le contenu de l'image recadrée, ce qui pourrait exposer un contenu sensible qui n'aurait jamais dû être rendu public. Mais, quelle que soit la manière dont l'image est créée, si l'image affectée ne soit pas partagée, le risque que la faille soit exploitée est faible, à moins que l'appareil ne soit pas compromis.

Pour installer les mises à jour de sécurité, l'utilisateur doit accéder à Microsoft Store > Libary > Get Updates, et la dernière version de Windows Snipping Tool sera automatiquement installée.

Après l'installation de la mise à jour de sécurité, Windows 11 Snipping Tool sera la version 10.2008.3001.0, et Windows 10 Snip & Sketch sera la version 11.2302.20.0.

Source : https://bit.ly/3LQm6DP

Cisco

Cisco corrige des vulnérabilités de haute gravité dans le logiciel IOS

23 Mars 2023

Cisco a publié son ensemble semestriel d'avis de sécurité pour les logiciels IOS et IOS XE, qui traite dix vulnérabilités, dont six classées comme étant de "haute gravité".

Répertoriée sous le nom de CVE-2023-20080, la première de ces failles concerne une validation insuffisante des limites de données permet à un attaquant d'envoyer des messages DHCPv6 des logiciels IOS et IOS XE fabriqués à un appareil affecté et de le recharger de manière inattendue.

La seconde vulnérabilité, CVE-2023-20072, a un impact sur le code de gestion de la fragmentation des paquets du protocole de tunnel et peut être exploitée en envoyant des paquets fragmentés fabriqués à un système affecté.

Cisco a également corrigé la vulnérabilité CVE-2023-20027, un problème dans l'implémentation de la fonction de réassemblage de la fragmentation virtuelle IPv4 (VFR) des logiciels IOS et IOS XE.

CVE-2023-20067 est une autre faille DoS de haute sévérité a été résolue dans la fonction de profilage client basée sur HTTP du logiciel IOS XE pour les contrôleurs LAN sans fil (WLC).

Cisco a également remédié à une validation d'entrée insuffisante dans le CLI du logiciel IOS XE SD-WAN.

Repéré comme CVE-2023-20035, ce bogue pourrait permettre à un attaquant disposant de privilèges limités de prendre le contrôle d'un système vulnérable.

La sixième faille est CVE-2023-20065, un problème de restrictions insuffisantes dans le sous-système d'hébergement d'applications IOx du logiciel IOS XE, qui pourrait permettre à un attaquant authentifié d'élever ses privilèges jusqu'à ceux de root.

Les mises à jour des logiciels IOS et IOS XE de Cisco comprennent également des correctifs pour des vulnérabilités de moyenne gravité en matière de déni de service, de traversée de chemin et d'élévation de privilèges.

Cisco a également publié des correctifs pour trois autres failles de gravité élevée, notamment un problème de démarrage sécurisé dans les commutateurs de la série Catalyst 9300, un bogue d'escalade des privilèges dans DNA Center et une vulnérabilité DoS dans le logiciel des points d'accès (AP).

Plusieurs problèmes de gravité moyenne ont été résolus dans le logiciel SD-WAN vManage, DNA Center, Adaptive Security Appliance (ASA), Firepower Threat Defense (FTD), les logiciels IOS et IOS XE, et le logiciel AP.

Cisco affirme ne pas avoir connaissance de l'exploitation de ces failles dans le cadre d'attaques malveillantes. Des informations supplémentaires sur les vulnérabilités résolues sont disponibles sur la page de sécurité des produits de Cisco.

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

Android

Les mises à jour d'Android corrigent plus de 50 vulnérabilités

07 Mars 2023

Google a annoncé des correctifs pour plus de 50 vulnérabilités dans le cadre des mises à jour de sécurité de mars 2023 pour la plateforme Android.

Les plus graves d'entre elles sont deux failles d'exécution de code à distance (RCE) dans le composant Système, qui ont toutes les deux été corrigés dans le cadre du niveau de correctif de sécurité 2023-03-01.

Au total, 18 bogues ont été corrigés dans le composant Système. Google a également résolu huit défauts de sécurité dans le composant Framework, tous classés comme étant de gravité "élevée".

Vingt-neuf autres vulnérabilités ont été résolues avec la deuxième partie des mises à jour Android du 2023-03-05.

Ces vulnérabilités concernent le noyau Android, les composants MediaTek, Unisoc, Qualcomm et Qualcomm closed-source. La plupart des problèmes sont des failles de haute sévérité, à l'exception de deux bogues dans les composants à source fermée de Qualcomm, qui sont classés "critiques".

Source : *https://bit.ly/42NDfUF*

Chrome

La mise à jour de sécurité d'iOS corrige une vulnérabilité exploitée dans les anciens iPhones

28 Mars 2023

Apple a annoncé de nouvelles mises à jour de sécurité pour macOS et iOS, y compris des correctifs qui corrigent une vulnérabilité exploitée dans les anciens modèles d'iPhone.

Le problème est sous le nom de CVE-2023-23529, a été initialement résolu en tant que zero-day à la mi-février, avec la publication d'iOS et iPadOS 16.3.1 et de macOS Ventura 13.2.1.

Impactant WebKit, la faille peut conduire à l'exécution de code arbitraire lors du traitement de contenu web malicieusement conçu et a été corrigée avec des vérifications améliorées.

Les correctifs sont inclus dans iOS 15.7.4 et iPadOS 15.7.4, qui sont déployés sur tous les modèles d'iPhone 6s et iPhone 7, iPhone SE de première génération, iPad Air 2, iPad mini de quatrième génération et iPod touch de septième génération.

La mise à jour de sécurité contient des correctifs pour un total de 16 vulnérabilités qui pourraient conduire à des fuites d'informations, à l'écriture de la mémoire, à l'exécution de code arbitraire, à l'usurpation de serveur VPN et à l'utilisation de données sensibles de l'utilisateur.

Apple a également publié des mises à jour pour les modèles d'iPhone et d'iPad de dernière génération, afin de corriger un total de 33 vulnérabilités. Présentées sous la forme d'iOS 16.4 et d'iPadOS 16.4, les mises à jour de la plateforme apportent également plusieurs améliorations à l'expérience utilisateur.

Près de 60 vulnérabilités ont été corrigées avec la publication de macOS Ventura 13.3. macOS Monterey 12.6.4 et Big Sur 11.7.5 ont été publiés avec des correctifs pour plus de 25 vulnérabilités chacun.

Apple a également corrigé deux vulnérabilités avec la publication de Safari 16.4, qui est disponible pour les utilisateurs de macOS Big Sur et macOS Monterey.

Des mises à jour de sécurité sont également disponibles pour tvOS et watchOS, ainsi que pour le micrologiciel Studio Display pour macOS Ventura. De plus amples informations sur les vulnérabilités corrigées sont disponibles sur le site web d'assistance d'Apple.

Source : *https://bit.ly/40MeKp3*

Actualité

Python : Un package malveillant peut échapper à la détection et voler des données

Un package Python malveillant du dépôt Python Package Index (PyPI) utilise l'Unicode pour échapper à la détection et déployer un logiciel malveillant permettant de voler des informations.

Le package concerné, nommé onyxproxy, a été téléchargé sur PyPI et permet de collecter et d'exfiltrer des informations d'identification et d'autres données précieuses. Depuis, il a été supprimé, mais pas avant d'avoir attiré un total de 183 téléchargements.

La société Phylum, spécialisée dans la sécurité de la chaîne d'approvisionnement des logiciels, indique que le logiciel intègre son comportement malveillant dans un script d'installation qui contient des milliers de chaînes de code apparemment légitimes.

Ces chaînes, qui mélangent des caractères forts et italiques, peuvent encore être lues et analysées par l'interpréteur Python, mais elles ne servent qu'à déclencher l'exécution du logiciel malveillant lors de l'installation du package.

Cela est possible grâce à l'utilisation de variantes Unicode de ce qui semble être le même caractère (également appelé homoglyphe) pour camoufler ses vraies couleurs (par exemple, self vs. **s***elf*) parmi des fonctions et des variables d'apparence inoffensive.

L'utilisation d'Unicode pour injecter des vulnérabilités dans le code source a déjà été révélée par les chercheurs de l'université de Cambridge Nicholas Boucher et Ross Anderson dans une technique d'attaque baptisée Trojan Source.

Cette nouvelle découverte démontre les efforts continus des acteurs de la menace pour développer de nouvelles techniques permettant de contourner les défenses basées sur la correspondance des chaînes de caractères en utilisant "la façon dont l'interpréteur Python utilise l'Unicode pour déguiser leurs logiciels malveillants".

Selon la société canadienne de cybersécurité PyUp, trois nouveaux paquets Python frauduleux ont été découverts : Aiotoolbox, asyncio-proxy et pycolorz. Ces paquets ont été téléchargés plus de 1 000 fois au total et avaient pour but de récupérer du code obscurci à partir d'un serveur distant.

Source : *https://bit.ly/40Wk7lo*

Une nouvelle arnaque sur Instagram utilise de fausses cartes-cadeaux SHEIN

Les chercheurs d'Avast ont détecté une nouvelle arnaque ciblant les utilisateurs d'Instagram de différents pays, notamment le Royaume-Uni, l'Australie, la France, l'Algérie, l'Espagne et la Pologne.

Cette arnaque sur les médias sociaux commence par un commentaire d'un utilisateur inconnu sur la publication d'une victime, la félicitant et lui disant qu'elle a été choisie comme l'un des 2023 heureux bénéficiaires d'une carte-cadeau SHEIN.

Les pirates offrent à l'utilisateur un lien vers leur profil Instagram, et à la fin, ils mentionnent une longue liste d'utilisateurs d'Instagram qui seront informés de la mention pour être attirés en tant que victimes de cette arnaque.

Un lien est visible sur le profil Instagram de l'attaquant, qui mène à un questionnaire de trois questions, il est important de noter que les réponses données n'ont pas d'importance : ce sont toujours les bonnes.

La victime se voit alors proposer neuf cases fermées parmi lesquelles elle doit choisir. Comme à l'étape précédente, peu importe les réponses choisies, la première sera toujours un échec et la seconde sera toujours gagnante.

La victime doit évidemment payer une petite somme d'argent pour recevoir son prix, ensuite elle est dirigée vers une page web où elle doit fournir certaines informations personnelles ainsi celles relatives à sa carte de crédit.

La victime s'attend à recevoir une carte-cadeau d'une valeur de plusieurs centaines d'euros ou de dollars, et c'est là que la fraude se produit. Bien qu'il semble qu'elle doive payer une petite somme pour l'acquérir, elle devient en réalité abonnée à un service dont elle ignore l'existence. Par exemple, en Australie, la victime doit payer 2 dollars australiens en plus de 69 dollars australiens toutes les deux semaines. En France, le coût est de 2 euros plus 33 euros toutes les deux semaines. Dans certains pays, le montant de la taxe n'est même pas publié. Bien entendu, aucun d'entre eux ne recevra la carte-cadeau.

Sans le vouloir, la victime consent à s'inscrire à un service d'abonnement dont elle ne sait rien.

Il existe un certain nombre de stratégies simples pour éviter les nombreuses nouvelles fraudes de ce type qui ne cessent d'apparaître sur les médias sociaux.

En plus d'être vigilant, il est conseillé d'installer un logiciel antivirus sur les appareils afin d'être alerté en cas d'accès à une page malveillante.

Source : *https://bit.ly/42WAqkb*

Fausse extension Chrome "FakeGPT" détournant les comptes Facebook

Guardio Labs (une startup spécialisée dans la cybersécurité) a découvert une nouvelle variante du voleur de comptes Facebook Ads depuis la découverte de FakeGPT, la fausse extension Chrome ChatGPT. Chaque jour, des milliers d'utilisateurs sont visés. Cette version se dissimule sous la forme d'un programme open-source contenant du code malveillant, ce qui la rend difficile à identifier.

L'extension malveillante, connue sous le nom de "Chat GPT for Google", est diffusée depuis le 14 mars via des résultats de recherche ChatGPT 4 sponsorisés sur Google.

Elle peut voler les cookies de session de Facebook et compromettre les comptes en ligne.

Les cookies sont ensuite envoyés au serveur des attaquants via une requête GET. La liste des cookies est cryptée par AES et jointe à la valeur de l'en-tête HTTP X-Cached-Key. Cela permet de s'assurer que les cookies peuvent être volés sans qu'aucun mécanisme d'inspection approfondie des paquets ne déclenche d'alarme.

Plus de 9 000 personnes avaient téléchargé l'extension FakeGPT au moment où elle a été retirée du Google Play Store.

Basée sur un code réel, cette version de FakeGPT n'exécute qu'une seule commande malveillante. Elle filtre les cookies liés à Facebook, les crypte en AES et les renvoie au serveur de l'attaquant.

Les acteurs de la menace peuvent utiliser les profils compromis comme bot pour promouvoir des services ou créer des pages et des comptes publicitaires.

Après avoir pris le contrôle d'un profil Facebook, l'attaquant a la possibilité de modifier l'identité et la photo du profil, de collecter des informations personnelles et de les utiliser à d'autres fins malveillantes.

Récemment, de nombreux utilisateurs sont tombés dans le piège, ce qui a augmenté le nombre de propagandes et d'activités malveillantes au sein de l'écosystème Facebook.

La popularité de ChatGPT est de plus en plus exploitée, et cette attaque n'est pas la seule. Il est recommandé aux utilisateurs d'Internet, même à domicile, de mettre en œuvre des services de protection et de détection de la sécurité. Ces services peuvent remédier aux importantes lacunes de sécurité qui affectent un grand nombre d'utilisateurs.

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

Bon à savoir

Les logiciels malveillants d'exfiltration deviennent un problème majeur en matière de cybersécurité

SpyCloud affirme que l'un des principaux facteurs de l'exposition continue des utilisateurs est l'augmentation des logiciels malveillants spécialement conçus pour voler des données directement à partir des ordinateurs et des navigateurs web.

Selon l'estimation de 2023, plus de 22 millions d'appareils différents ont été infectés par des logiciels malveillants. Environ 50 % des 721,5 millions d'informations d'identification exposées que SpyCloud a pu récupérer provenaient de botnets.

Selon Trevor Hilligoss, directeur de la recherche en sécurité chez SpyCloud, "l'utilisation généralisée des infostealers est une tendance dangereuse car ces attaques ouvrent la voie à des acteurs malveillants tels que les Initial Access Brokers, qui vendent des journaux de logiciels malveillants contenant des données d'authentification précises à des syndicats de ransomware et à d'autres criminels."

Lorsque les employés accèdent aux réseaux d'entreprise à l'aide d'appareils non gérés ou mal gérés infectés par des logiciels malveillants, les acteurs de la menace ont un moyen facile d'accéder aux applications professionnelles critiques, y compris les plateformes d'authentification unique et les réseaux privés virtuels.

Les chercheurs de SpyCloud ont récupéré des millions d'informations d'identification provenant d'applications professionnelles qui ont été compromises par des logiciels malveillants en 2022. Les fuites de données de ces applications, qui comprennent des référentiels de code, des bases de données clients, des services de messagerie et des systèmes de ressources humaines, fournissent aux attaquants les connaissances dont ils ont besoin pour lancer des attaques de suivi préjudiciables telles que des ransomwares.

Même une fois que l'appareil a été nettoyé des logiciels malveillants, si ces informations d'identification ne sont pas correctement corrigées et restent actives, elles continueront à représenter une menace pour les organisations.

"Collectivement, nous devons commencer à penser à la protection des identités numériques en utilisant une approche de remédiation post-infection, plutôt que de nous concentrer uniquement sur le nettoyage des appareils infectés. Agir sur les données exposées des employés avant qu'elles ne puissent être utilisées par des criminels est primordial pour prévenir la prise de contrôle des comptes, la fraude, les ransomwares et d'autres formes de cybercriminalité", a déclaré M. Hilligoss.

Malgré l'attention accordée à la formation en matière de cybersécurité, les mots de passe sont encore mal utilisés : 72 % des utilisateurs touchés par des violations en 2022 ont continué à utiliser des informations d'identification qui avaient déjà été compromises.

Le secteur public est plus exposé aux risques liés aux appareils infectés par des logiciels malveillants que les entreprises : SpyCloud a découvert 695 violations contenant des courriels .gov en 2022, soit une augmentation de près de 14 % par rapport à 2021. Les taux de réutilisation des mots de passe parmi les employés du gouvernement restent élevés.

'123456', '12345678' et 'password' sont les trois mots de passe en clair exposés les plus fréquemment utilisés dans les communications officielles du gouvernement.

Source : *https://bit.ly/42Zsdvx*

Evènements

Evènement du mois

Passer au « sans mot de passe » : l'avenir de la cybersécurité

30 Mars 2023

Online

https://bit.ly/3ZuMDJP

Les mots de passe sont progressivement abandonnés et un avenir sans mot de passe se profile à l'horizon. L'augmentation des cybermenaces et une mauvaise hygiène des mots de passe continuent de poser des risques pour les organisations qui utilisent des mots de passe. L'authentification sans mot de passe renforce la sécurité en éliminant les pratiques risquées de gestion des mots de passe et en réduisant les vecteurs d'attaque.

Dans ce webinaire, ils ont partagé les meilleures pratiques de déploiement sans mot de passe pour répondre aux exigences de sécurité.

Evènement à venir

Fraude et compromission par e-mail professionnel

01 Avril 2023

Online

https://bit.ly/3JUGNfi

La cybersécurité sur le lieu de travail est devenue de plus en plus critique à mesure que de plus en plus d'organisations migrent vers les services cloud.

Alors que l'adoption des canaux numériques et les initiatives de travail à domicile ont connu une croissance exponentielle, le nombre d'attaques de phishing, de fraudes par e-mail professionnel, de violations de données et d'attaques de ransomwares a également augmenté.

Il est essentiel d'aborder cette formation en ligne de sensibilisation à la sécurité pour être prête à faire face aux cybermenaces.

Référence	ANPT-2023-BV-03
Titre	Bulletin de veille N°03
Date de version	31 Mars 2023
Contact	ssi@anpt.dz