BULLETIN DE VEILLE N°11

ANPT-2022-BV-11

" Quantum Encryption is essential to protect our digital assets and infrastructure from attackers."
-- Kevin Coleman--

Novembre 2022

Alertes de sécurité

Chrome

Chrome : Une mise à jour d'urgence pour corriger la huitième journée Zero-Day de 2022

25 Novembre 2022

Google a publié une mise à jour de sécurité d'urgence pour la version de bureau du navigateur Web Chrome, qui corrige la huitième vulnérabilité de type "zero-day" exploitée dans des attaques cette année.

La faille de haute gravité est suivie sous le nom de CVE-2022-4135, c'est un débordement de tampon de tas dans GPU, découvert par Clément Lecigne du groupe d'analyse des menaces de Google le 22 novembre 2022.

Comme les utilisateurs ont besoin de temps pour appliquer la mise à jour de sécurité sur leurs installations Chrome, Google n'a pas divulgué de détails sur la vulnérabilité pour éviter d'étendre son exploitation malveillante.

Les attaquants peuvent utiliser le débordement de tampon de tas pour écraser la mémoire d'une application et manipuler son chemin d'exécution, ce qui entraîne un accès illimité aux informations ou une exécution de code arbitraire.

Il est recommandé aux utilisateurs de Chrome de passer à la version 107.0.5304.121/122 pour Windows et 107.0.5304.122 pour Mac et Linux.

Source : *https://bit.ly/3GRjwe1*

VMware

VMware signale 3 nouvelles failles critiques affectant le logiciel d'assistance Workspace ONE

09 Novembre 2022

VMware a corrigé cinq failles de sécurité affectant sa solution Workspace ONE Assist, dont certaines pourraient être exploitées pour contourner l'authentification et obtenir des autorisations élevées.

Les chercheurs en sécurité Jasper Westerman, Jan van der Put, Yanick de Pater et Harm Blankers, de la société néerlandaise Reqon, ont découvert et signalé ces failles.

En tête de liste figurent trois bogues (score CVSS est 9.8) :

- CVE-2022-31685 est une faille de contournement d'authentification qui pourrait être exploitée par un attaquant disposant d'un accès réseau à VMware Workspace ONE Assist pour obtenir un accès administratif sans avoir à s'authentifier auprès de l'application.
- CVE-2022-31686 est une vulnérabilité "Broken Authentication Method".
- CVE-2022-31687 est une faille de "Broken Access Control".

Une vulnérabilité XSS (cross-site scripting) reflétée (CVE-2022-31688, score CVSS : 6.4) provenant d'une mauvaise vérification des Users-Input, ce qui pourrait être exploité pour injecter du code JavaScript arbitraire dans la fenêtre de l'utilisateur cible.

Le patch se termine par une vulnérabilité de fixation de session (CVE-2022-31689, score CVSS : 4,2) qui, selon VMware, résulte d'une mauvaise gestion des jetons de session.

Tous les problèmes concernent les versions 21.x et 22.x de VMware Workspace ONE Assist ont été corrigés dans la version 22.10. La société a également déclaré qu'il n'y a pas de solutions de contournement pour remédier à ces faiblesses.

Source : *https://bit.ly/3Xzgn1H*

Microsoft

La dernière mise à jour de Windows. Correctifs publiés pour 6 "Zero-Days" activement exploités

09 Novembre 2022

Microsoft a publié des correctifs pour 68 vulnérabilités couvrant son portefeuille de logiciels, y compris des correctifs pour six "zero-days" activement exploités.

Douze de ces problèmes sont jugés critiques, deux sont jugés élevés et 55 sont jugés importants en termes de gravité. Ces chiffres incluent également les faiblesses qui ont déjà été corrigées par OpenSSL.

CVE-2022-3723 est une faille activement exploitée dans les navigateurs basés sur Chromium et qui a été traitée dans Microsoft Edge au début du mois.

Deux anciennes CVEs de type "zero-day" affectant Exchange Server, rendues publiques fin septembre, ont finalement été corrigées. Alors il est conseillé aux clients de mettre à jour leurs systèmes Exchange Server immédiatement.

Les vulnérabilités activement exploitées sont :

- CVE-2022-41040 (score CVSS : 8.8) et CVE-2022-41082 (score CVSS : 8.8) - Vulnérabilités d'élévation de privilèges de Microsoft Exchange Server (alias ProxyNotShell).
- CVE-2022-41128 (score CVSS : 8.8) - Vulnérabilité d'exécution de code à distance des langages de script Windows, et qui réside dans le composant JScript9 et se produit lorsqu'une cible est amenée à visiter un site Web spécialement conçu.
- CVE-2022-41125 (score CVSS : 7.8) - Vulnérabilité d'élévation de privilège du service d'isolation de clé CNG de Windows.
- CVE-2022-41073 (score CVSS : 7.8) - Vulnérabilité d'élévation de privilège dans le spouleur d'impression de Windows.
- CVE-2022-41091 (score CVSS : 5.4) - est l'une des deux failles de contournement de la fonction de sécurité Mark Of The Web de Windows, elle était utilisée par le ransomware Magniber pour cibler les utilisateurs avec de fausses mises à jour logicielles. La deuxième faille MotW à être résolue est CVE-2022-41049 (alias ZippyReads), elle est liée à l'absence de définition de l'indicateur Mark of the Web pour les fichiers d'archive extraits.

Quatre autres bogues classés critiques méritent d'être signalés : des failles d'élévation de privilèges dans Windows Kerberos (CVE-2022-37967), Kerberos RC4-HMAC (CVE-2022-37966) et Microsoft Exchange Server (CVE-2022-41080), ainsi qu'une faille DOS affectant Windows Hyper-V (CVE-2022-38015).

La liste des correctifs pour les failles critiques est complétée par quatre bogues d'exécution de code à distance dans le protocole PPTP (Point-to-Point Tunneling Protocol), qui ont toutes un score CVSS de 8.1 (CVE-2022-41039, CVE-2022-41088 et CVE-2022-41044), et une autre qui affecte les langages de script Windows JScript9 et Chakra (CVE-2022-41118).

La mise à jour du Patch résout également un certain nombre de failles d'exécution de code à distance dans Microsoft Excel, Word, ODBC Driver, Office Graphics, SharePoint Server et Visual Studio, ainsi qu'une poignée de bogues d'élévation de privilèges dans Win32k, Overlay Filter et Group Policy.

Source : *https://bit.ly/3gC9nYd*

Microsoft publie une mise à jour hors bande après avoir des problèmes avec Kerberos

22 Novembre 2022

Quelques jours après la publication de la mise à jour du Patch qui traite la vulnérabilité d'élévation de privilèges qui affectant Windows Server, les utilisateurs ont commencé à se plaindre de problèmes liés à l'authentification Kerberos CVE-2022-37966. Cette faille de haute gravité peut permettre à un attaquant qui peut collecter des informations sur le système ciblé d'obtenir des privilèges d'administrateur.

Microsoft a fourni des mesures d'atténuation quelques jours plus tard. Puis, elle a publié une mise à jour hors bande qui devrait résoudre le problème.

CVE-2022-37966 n'a pas été exploité dans la nature, mais Microsoft lui a attribué la mention "exploitation plus probable".

Source : *https://bit.ly/3Vew8Aq*

Apple

Apple corrige des failles d'exécution de code à distance dans iOS et macOS

10 Novembre 2022

Apple a publié des correctifs hors bande pour iOS et macOS, afin de corriger deux vulnérabilités d'exécution de code arbitraire dans la bibliothèque libxml2.

Écrit en langage de programmation C et développé à l'origine pour le projet Gnome, libxml2 est une bibliothèque logicielle permettant d'analyser des documents XML.

Repérées sous les noms de CVE-2022-40303 (l'absence de limitations spécifiques pourrait conduire à des débordements d'entiers) et CVE-2022-40304 (des erreurs de mémoire telles que des bogues double-free), les deux vulnérabilités pourraient conduire à l'exécution de code à distance.

Apple a corrigé les failles avec la publication de macOS Ventura 13.0.1 et iOS 16.1.1 et iPadOS 16.1.1 (pour iPhone 8 et ultérieur, iPad Pro (tous les modèles), iPad Air 3e génération et ultérieur, iPad 5e génération et ultérieur, et iPad mini 5e génération et ultérieur).

Source : *https://bit.ly/3ubp2Ra*

Cisco

Les vulnérabilités Cisco ISE peuvent être enchaînées en un clic

28 Novembre 2022

Quatre vulnérabilités dans Cisco Identity Services Engine (ISE) ont été identifiées, l'exploitation de toutes ces failles nécessitant qu'un attaquant soit un utilisateur valide et autorisé du système ISE.

La plus grave de ces vulnérabilités est CVE-2022-20964, un bogue d'injection de commande dans la fonctionnalité tcpdump de l'interface de gestion Web d'ISE. Le bogue de gravité élevée existe car l'entrée utilisateur n'est pas correctement validée.

- CVE-2022-20959 est une faille XSS dans ISE, un attaquant pourrait facilement obtenir un shell racine distant sur le système vulnérable.
- CVE-2022-20966 et CVE-2022-20967 ont été identifiées dans les fonctionnalités tcpdump et External RADIUS Server de l'interface de gestion Web.

Cisco indique que des correctifs sont prévus pour le premier trimestre de 2023, sous la forme des versions 3.1p6 et 3.2p1 de Cisco ISE.

Source : *https://bit.ly/3Uh6SrO*

Actualité

Des faux comptes Facebook et Instagram liés à une opération d'influence pro-américaine sont éliminés par Meta !

Meta Platforms a annoncé avoir éliminé un réseau de profils et de pages Facebook et Instagram qui étaient utilisés par des individus liés à l'armée américaine pour diffuser des histoires qui présentaient la nation de manière favorable à travers le Moyen-Orient et l'Asie centrale.

L'Afghanistan, l'Algérie, l'Iran, l'Irak, le Kazakhstan, le Kirghizistan, la Russie, la Somalie, la Syrie, le Tadjikistan, l'Ouzbékistan et le Yémen étaient les principales cibles du réseau, qui avait ses racines aux États-Unis.

Selon le géant des médias sociaux, les auteurs de cette activité se sont fait passer pour des membres des communautés qu'ils ont ciblées, diffusant des contenus en arabe, en farsi et en russe qui prônent une plus grande coopération militaire avec les États-Unis et dénigrent la Chine, l'Iran et la Russie.

Dans son rapport trimestriel sur la menace adverse, Meta a indiqué que ces scénarios comprenaient "l'invasion de l'Ukraine par la Russie, le traitement du peuple ouïghour par la Chine, l'influence de l'Iran au Moyen-Orient et le soutien du régime taliban en Afghanistan par la Russie et la Chine".

Des documents sur l'épidémie de COVID-19 ont également été mis en ligne, dont certains ont été retirés par l'entreprise pour avoir enfreint sa politique de désinformation.

En outre, les faux comptes ont affiché leurs photos de profil à l'heure normale de l'Est (EST) plutôt qu'aux heures ouvrables dans les pays ciblés, en employant vraisemblablement des méthodes d'apprentissage automatique comme les réseaux adversatifs génératifs (GAN).

Jusqu'à 39 comptes Facebook, 16 pages, 2 groupes et 26 comptes Instagram ont été découverts comme présentant un comportement faux coordonné. Les autres plateformes concernées par l'opération étaient Twitter, YouTube, Telegram, VKontakte et Odnoklassniki.

En ce qui concerne la portée, Meta a découvert que plus de 22 000 comptes suivaient un ou plusieurs de ces sites, 400 ont rejoint au moins un Groupe, et environ 12 000 utilisateurs ont suivi un ou plusieurs comptes Instagram. Les publicités sur Facebook ont coûté environ 2 500 dollars et ont été achetées à la fois en monnaie américaine et en livres sterling.

Cependant, il semble que les tentatives aient été principalement inefficaces. La majorité des messages de cette opération n'ont reçu que peu ou pas d'interaction de la part des communautés réelles, selon Meta.

Les chercheurs de Graphika et du Stanford Internet Observatory ont découvert au début du mois d'août que la campagne utilisait plusieurs plates-formes de médias sociaux pour diffuser des récits pro-occidentaux.

Le Stanford Internet Observatory a noté qu'il s'agissait du "cas le plus important d'opérations secrètes d'influence pro-occidentale sur les médias sociaux" et que "ces campagnes ont constamment mis en avant des récits promouvant les intérêts des États-Unis et de leurs alliés tout en s'opposant à des pays comme la Russie, la Chine et l'Iran".

***Source** : https://bit.ly/3ui9ACN*

Les dépôts de Docker Hub cachent plus de 1 650 conteneurs malveillants

Plus de 1 600 images Docker Hub accessibles au public dissimulent des activités malveillantes, telles que des mineurs de crypto-monnaies, des données implantées pouvant être exploitées comme des portes dérobées, des détourneurs de DNS et des redirecteurs de sites Web.

Les images Docker servent de modèles pour construire rapidement et facilement des conteneurs avec du code et des applications préconstruits. Par conséquent, les personnes souhaitant lancer de nouvelles instances utilisent fréquemment Docker Hub pour découvrir une application qui peut être déployée rapidement.

Malheureusement, plus d'un millier de téléchargements malveillants présentent de graves dangers pour les utilisateurs non avertis qui déploient des images remplies de logiciels malveillants sur des conteneurs hébergés localement ou dans le nuage, suite à l'utilisation abusive du service par des acteurs de la menace.

Les acteurs de la menace ont publié plusieurs photos infectées avec des noms qui les font apparaître comme des projets connus et fiables afin de tromper les consommateurs et les inciter à les télécharger.

Les chercheurs de Sysdig ont étudié le problème, en essayant d'évaluer sa portée et ont signalé les images découvertes qui incluent un mécanisme ou un code malveillant.

Sysdig a utilisé ses scanners automatiques pour examiner 250 000 images Linux non vérifiées et a identifié 1 652 d'entre elles comme étant malveillantes.

La plus grande catégorie était celle des crypto-miners, trouvée dans 608 images de conteneurs, ciblant les ressources du serveur pour miner de la crypto-monnaie pour les acteurs de la menace.

Les images avec des secrets codés étaient la deuxième occurrence la plus fréquente, représentant 281 instances. Ces images contiennent des clés SSH, des informations de connexion AWS, des jetons GitHub, des jetons NPM et d'autres secrets.

Selon Sysdig, ces secrets peuvent avoir été laissés sur des images publiques par erreur ou injectés intentionnellement par l'acteur de la menace qui les a créés et téléchargés.

"En intégrant une clé SSH ou une clé API dans le conteneur, l'attaquant peut obtenir un accès une fois le conteneur déployé", prévient Sysdig dans le rapport. "Par exemple, le téléchargement d'une clé publique sur un serveur distant permet aux

propriétaires de la clé privée correspondante d'ouvrir un shell et d'exécuter des commandes via SSH, ce qui revient à implanter une porte dérobée."
Le typosquattage a été largement utilisé par les images malveillantes pour se faire passer pour des images fiables et légitimes afin d'infecter les utilisateurs avec des crypto-miners.
Sysdig indique qu'en 2022, 61% de toutes les images extraites de Docker Hub proviennent de référentiels publics, soit une augmentation de 15% par rapport aux statistiques de 2021, de sorte que le risque pour les utilisateurs est à la hausse.

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

5,4 millions de données volées de Twitter ont été divulguées en ligne et d'autres ont été partagées en privé

Un forum de pirates a révélé que plus de 5,4 millions d'enregistrements d'utilisateurs de Twitter contenant des informations privées avaient été obtenus en exploitant une faille de l'API qui avait été corrigée en janvier.
Un chercheur en sécurité a également révélé un autre déversement de données énorme, peut-être plus important, de millions d'enregistrements Twitter, montrant à quel point cette faille a été utilisée par les acteurs de la menace.
Les données sont constituées d'informations publiques récupérées ainsi que de numéros de téléphone et d'adresses électroniques privés qui ne sont pas censés être publics.
La majorité du contenu était constituée de détails accessibles au public, tels que des identifiants Twitter, des noms, des noms de connexion, des localités et des statuts vérifiés ; cependant, il y avait aussi des informations privées dont des numéros de téléphone et des adresses électroniques.
Ces informations ont été recueillies en décembre 2021 grâce à une faille dans l'API de Twitter, rendue publique par le programme de primes aux bugs de HackerOne. Cette faille permettait aux utilisateurs de soumettre leurs numéros de téléphone et leurs adresses électroniques à l'API afin d'obtenir l'identifiant Twitter correspondant.
À l'aide de cet identifiant, les acteurs de la menace peuvent ensuite récupérer les données publiques disponibles sur le compte pour produire l'enregistrement d'un nouvel utilisateur.
Twitter a confirmé avoir subi une violation de données due à un problème d'API résolu en janvier 2022.
Pompompurin, le propriétaire du site de piratage Breached, a révélé qu'il était chargé d'exploiter la faille et de produire l'énorme décharge de données d'utilisateurs de Twitter après qu'un autre acteur de la menace répondant au nom de "Devil" lui ait révélé la vulnérabilité.
Près de 7 millions de profils Twitter contenant des informations privées ont été découverts au total, y compris les 5,4 millions d'enregistrements mis en vente et 1,4 million de profils d'utilisateurs suspendus supplémentaires qui ont été recueillis via une autre API.
Pompompurin a précisé que cette deuxième décharge de données n'a été distribuée à titre privé qu'à un groupe restreint de personnes et n'a pas été vendue.
Bien qu'il soit troublant que les acteurs de la menace aient communiqué 5,4 millions d'enregistrements, il est également affirmé que la même vulnérabilité a été utilisée pour créer une décharge de données beaucoup plus importante.
Ce déversement de données pourrait comprendre des dizaines de millions d'enregistrements Twitter, y compris des données publiques telles que le statut vérifié, les noms de comptes, les identifiants Twitter, les biographies et les pseudonymes, ainsi que des numéros de téléphone personnels recueillis à l'aide du même problème d'API.
L'expert en sécurité Chad Loder, qui a initialement signalé l'information sur Twitter et a été suspendu peu après l'avoir publiée, est à l'origine de l'information sur cette fuite de données plus grave. Plus tard, Loder a publié un échantillon de cette violation de données plus large sur Mastodon (un réseau social) avec des rédactions.
"Je viens de recevoir la preuve d'une violation massive des données de Twitter affectant des millions de comptes Twitter dans l'UE et aux États-Unis. J'ai contacté un échantillon des comptes concernés et ils ont confirmé que les données violées sont exactes. Cette violation a eu lieu au plus tôt en 2021", a déclaré Chad Loder sur Twitter.

La fuite de données inconnues de Twitter, qui contient 1 377 132 numéros de téléphone d'utilisateurs en France.
Les chercheurs ont confirmé avec de nombreux utilisateurs de cette fuite que les numéros de téléphone sont valides, vérifiant que cette violation de données supplémentaire est réelle.
En outre, aucun de ces numéros de téléphone n'est présent dans les données originales vendues en août, ce qui montre à quel point la violation de données de Twitter était beaucoup plus importante que ce qui avait été révélé précédemment et la grande quantité de données d'utilisateurs qui circulent parmi les acteurs de la menace.

Source : *https://bit.ly/3u9lnUb*

Bon à savoir

La Coupe du monde de la FIFA attire les cybercriminels

La coupe du monde de la FIFA a attiré le public du monde entier dont les cybercriminels qui veulent profiter des diverses bases de fans et des organisations participantes pour gagner rapidement de l'argent.
Selon CloudSEK, les dangers pour les entreprises et le public comprennent les campagnes de menaces persistantes avancées (APT), le phishing, la fraude à la carte de crédit/aux crypto-monnaies, les assauts DDoS et le vol d'identité. Les cybercriminels sont motivés par le gain monétaire, l'idéologie ou les liens avec des groupes géopolitiques particuliers.
"Les cybercriminels ont profité du décalage entre l'offre et la demande de billets de match de la Coupe du monde de la FIFA, de billets d'avion, d'hôtels, de souvenirs, etc. pour escroquer les fans et les passionnés. Les utilisateurs devraient limiter leurs achats aux

sites web officiels et aux applications mobiles, malgré les offres alléchantes et les tentations. Les entreprises qui sponsorisent la FIFA devraient également renforcer leurs mesures de sécurité et se tenir au courant des stratégies utilisées par les acteurs de la menace, selon un chercheur de CloudSEK.

☞ Les fans de la FIFA sont conseillés a :

- Ne pas acheter les cartes Hayya et les billets FIFA que sur le site officiel ;
- Ne pas réaliser des transactions de crypto-monnaies, sans assurer leurs légitimités ;
- Ne pas utiliser les réseaux sociaux ou Telegram pour accéder aux services liés à la FIFA ;
- Ne jamais divulguer les informations personnelles identifiables (PII) ou les informations bancaires à des personnes ou des sites web non identifiés ;
- Ne pas installer des applications provenant de magasins d'applications tiers, de médias sociaux ou de Telegram.

☞ Recommandations pour les organisations participantes :

- Utiliser des équilibreurs de charge ou des services comme Cloudflare pour éviter les attaques DDoS ;
- Utiliser un pare-feu et maintenir les logiciels à jour dans leur dernière version ;
- Organiser des campagnes de sensibilisation pour informer les fans et les utilisateurs sur les portails et les sites Web légitimes ;
- Surveiller et supprimer en temps réel les sites de phishing, les fausses applications et les pages de médias sociaux copiées ;
- Signaler les résultats aux autorités compétentes qui peuvent prendre des mesures contre les acteurs de la menace.

Pour limiter les attaques potentielles dans cette coupe du monde, il faut respecter les mesures de sécurité par toute personne fan ou organisation participante.

Source : *https://bit.ly/3Ui826z*

Evènements

Evènement du mois

SECURA NORTH AFRICA ALGERIA 2022

22 - 24 Novembre 2022

SAFEX (Pavillon Union) Alger, Algérie

https://bit.ly/3VtQBB0

Le salon international Secura North-Africa ambitionne, dans sa quatrième édition, de contribuer à l'effort national dans la lutte contre les incendies, qu'ils soient domestiques, industriels ou feux de forêt.

Une centaine d'entreprises, algériennes à 90%, représentant 150 marques nationales et internationales, participent à ce salon dont l'ANPT était l'une de ces soutiens officiels.

L'objectif de cet événement est de rassembler au même endroit pendant 3 jours tous les acteurs et professionnels du secteur de la sécurité industrielle et commerciale, de la sécurité des travailleurs, de la lutte contre l'incendie et des urgences.

Evènement à venir

BLACK HAT EUROPE 2022

05-08 / 14 Novembre 2022

Londres / Online

https://bit.ly/3ENqVIY

Black Hat offre aux participants les dernières recherches, développements et tendances en matière de sécurité de l'information. Les professionnels et les chercheurs les plus brillants du secteur se réunissent pour un total de quatre jours - deux jours de formations pratiques très techniques, suivis de deux jours consacrés aux dernières recherches et divulgations de vulnérabilités dans les briefings.

L'événement sera en direct et en personne à Londres, du 5 au 8 décembre, suivi une semaine plus tard d'une expérience virtuelle comprenant des enregistrements de tous les briefings et des sessions sponsorisées, disponibles le 14 décembre.

Référence	ANPT-2022-BV-11
Titre	Bulletin de veille N°11
Date de version	30 Novembre 2022
Contact	ssi@anpt.dz