BULLETIN DE VEILLE N°10

ANPT-2022-BV-10

"To competently perform rectifying security service, two critical incident response elements are necessary: information and organization."
-- Robert E. Davis --

Octobre 2022

Alertes de sécurité

Cisco

Cisco avertit les administrateurs de corriger la faille AnyConnect exploitée dans les attaques

25 Octobre 2022

Cisco a averti ses clients que deux vulnérabilités de sécurité dans Cisco AnyConnect Secure Mobility Client pour Windows sont exploitées dans la nature.

Secure Mobility Client AnyConnect simplifie l'accès sécurisé aux terminaux d'entreprise et permet aux employés de travailler de n'importe où tout en étant connectés à un réseau privé virtuel (VPN) sécurisé via Secure Sockets Layer (SSL) et IPsec IKEv2.

Les deux failles de sécurité (CVE-2020-3433 et CVE-2020-3153) permettent aux attaquants locaux de réaliser des attaques de détournement de DLL et de copier des fichiers dans des répertoires système avec des privilèges de niveau système.

Heureusement, les deux vulnérabilités nécessitent une authentification, les attaquants devant disposer d'informations d'identification valides sur le système. Cependant, elles pourraient être enchaînées avec des failles d'élévation de privilèges Windows, d'autant plus que des exploits de preuve de concept sont déjà disponibles en ligne pour les deux CVEs.

L'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a ajouté les deux failles de sécurité à son catalogue des vulnérabilités connues et exploitées. Toutes les agences fédérales civiles de l'exécutif (FCEB) sont tenues par une directive opérationnelle contraignante (BOD 22-01) d'appliquer des correctifs ou des mesures d'atténuation.

Comme l'a ajouté la CISA, ces types de failles constituent un vecteur d'attaque fréquent pour les cyberacteurs malveillants et présentent un risque important pour l'entreprise fédérale.

La CISA a recommandé à toutes les organisations du monde entier d'accorder la priorité à la correction de ces bogues de sécurité, même si le BOD 22-01 ne s'applique qu'aux agences FCEB américaines.

Source : *https://bit.ly/3SMI1eN*

Apple

Apple corrige plus de 100 vulnérabilités avec la publication de macOS Ventura 13

25 Octobre 2022

Apple a annoncé le lancement officiel de macOS Ventura 13, la 19ème version majeure de son système d'exploitation de bureau. En plus de plusieurs nouvelles fonctionnalités, macOS Ventura 13 apporte des correctifs pour plus de 100 vulnérabilités.

Au total, 112 identifiants CVE sont répertoriés dans l'avis de sécurité d'Apple pour macOS Ventura 13, y compris des problèmes spécifiques au système d'exploitation et des failles ayant un impact sur des composants tiers.

L'exploitation de ces vulnérabilités peut conduire à l'exécution de code arbitraire, à la divulgation d'informations, à un déni de service (DoS), à des modifications du système de fichiers, à des contournements de sécurité et à une élévation de privilèges.

Dans de nombreux cas, l'exploitation nécessite le déploiement d'applications malveillantes sur le système ciblé. Dans certains cas, une attaque nécessiterait un accès physique à l'appareil ou le traitement de fichiers malveillants.

Apple a également publié les mises à jour macOS Big Sur (11.7.1) et Monterey (12.6.1), qui corrigent trois des vulnérabilités corrigées par Ventura 13.

Apple a également annoncé avoir corrigé plus de 20 failles de sécurité avec la publication de mises à jour d'iOS et d'iPadOS, dont CVE-2022-42827, un Zero-day qui a été exploité dans des attaques. Aucune information n'a été communiquée sur les attaques exploitant CVE-2022-42827.

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

Adobe

Des failles critiques dans le Abode Home Security Kit

24 Octobre 2022

Abode Systems a résolu plusieurs vulnérabilités graves dans son Home-Security-Kit, y compris des problèmes critiques qui

pourraient permettre aux attaquants d'exécuter des commandes avec les privilèges de l'utilisateur root.

Les utilisateurs de Abode Systems peuvent contrôler le système via un site web ou une application sur leurs appareils mobiles, et l'intégrer à Amazon Alexa, Apple Homekit et Google Home.

Les chercheurs de Cisco Talos ont découvert que le kit de sécurité Iota all-in-one est affecté par des vulnérabilités qui pourraient permettre aux attaquants de modifier les mots de passe des utilisateurs, de changer la configuration des appareils, d'injecter du code arbitraire et même d'arrêter complètement le système. Un attaquant pourrait prendre le contrôle à distance des caméras ciblées ou les désactiver.

Au total, 14 vulnérabilités de gravité critique (score CVSS de 10) d'injection de commandes d'OS ont été identifiées dans Home Security Kit. Les chercheurs en sécurité de Cisco préviennent qu'elles pourraient être exploitées pour exécuter des commandes système arbitraires avec les privilèges de l'utilisateur root.

Trois autres failles critiques dans le kit d'Abode Systems sont décrites comme des bogues de Format String Injection, contournement d'authentification et Integer-Overflow.

Neuf des défauts de sécurité sont décrits comme des vulnérabilités de haute gravité d'injection de chaîne de format qui pourraient être exploitées en utilisant des requêtes HTTP, des XCMD ou des valeurs de configuration spécialement rédigées.

Les autres vulnérabilités de haute gravité identifiées dans le produit comprennent un contournement d'authentification, deux défauts d'injection de commande et un bogue double-free.

Il est conseillé aux utilisateurs de mettre à jour vers Iota 6.9X ou 6.9Z dès que possible.

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

Google

Google corrige la septième faille zero-day de Chrome exploitée dans des attaques cette année

28 Octobre 2022

Google a publié une mise à jour de sécurité d'urgence pour le navigateur Web de bureau Chrome afin de corriger une seule vulnérabilité connue pour être exploitée dans des attaques.

La faille de haute gravité (CVE-2022-3723) est un bogue de confusion de type dans le moteur Javascript Chrome V8 qui existe dans la nature, découvert et signalé à Google par les analystes d'Avast.

La société ne fournit pas beaucoup de détails sur la vulnérabilité pour des raisons de sécurité.

En général, les vulnérabilités de confusion de type se produisent lorsque le programme alloue une ressource, un objet ou une variable en utilisant un type et y accède ensuite en utilisant un type différent et incompatible, ce qui entraîne un accès à la mémoire hors limites.

En accédant à des parties de la mémoire qui ne devraient pas être accessibles dans le contexte de l'application, un attaquant pourrait lire des informations sensibles d'autres applications, provoquer des plantages ou exécuter du code arbitraire.

Google ne précise pas le niveau d'activité impliquant l'exploit qui existe dans la nature, de sorte que ce n'est pas encore claire si les attaques utilisant CVE-2022-3723 sont répandues ou limitées.

Il est donc vivement conseillé aux utilisateurs de Chrome de mettre à jour leur navigateur Web à la version 107.0.5304.87/88 dès que possible afin de bloquer les tentatives d'exploitation.

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

Juniper

Des failles de haute gravité dans le système d'exploitation Junos de Juniper affectent les équipements de réseau d'entreprise

28 Octobre 2022

De multiples failles de sécurité de haute gravité ont été révélées comme affectant les appareils Juniper Networks, dont certaines pourraient être exploitées pour permettre l'exécution de code.

La plus importante d'entre elles est une vulnérabilité de désérialisation de fichier d'archive PHP pré-authentifiée à distance (CVE-2022-22241, score CVSS : 8.1) dans le composant J-Web de Junos OS, selon Paulos Yibelo, chercheur chez Octagon Networks. Cette vulnérabilité peut être exploitée par un attaquant distant non authentifié pour obtenir des fichiers « PHAR » distants désérialisés, conduisant à une écriture de fichier arbitraire, ce qui conduit à une exécution de code à distance (RCE).

CVE-2022-22242 (score CVSS : 6.1) - Un XSS réfléchi pré-authentifié sur la page d'erreur ("error.php"), permettant à un adversaire distant de siphonner la session d'administration de Junos OS et enchaîné avec d'autres failles qui nécessitent une authentification.

CVE-2022-22243 (score CVSS : 4.3) & CVE-2022-22244 (score CVSS : 5.3) - Deux failles d'injection XPATH exploitées par un attaquant distant authentifié pour voler et manipuler les sessions d'administration de Junos OS.

CVE-2022-22245 (score CVSS : 4.3) - Une faille qui pourrait permettre à un attaquant distant authentifié de télécharger des fichiers PHP vers n'importe quel emplacement arbitraire.

CVE-2022-22246 (CVSS score : 7.5) - Une vulnérabilité d'inclusion de fichier local qui pourrait être utilisée pour exécuter du code PHP non approuvé, elle peut conduire aussi à l'exécution de code à distance.

Il est recommandé d'appliquer le dernier correctif logiciel disponible pour Junos OS afin d'atténuer les menaces susmentionnées.

Ces problèmes ont été corrigés dans les versions 19.1R3-S9, 19.2R3-S6, 19.3R3-S7, 19.4R3-S9, 20.1R3-S5, 20.2R3-S5, 20.3R3-S5, 20.4R3-S4, 21.1R3-S2, 21.3R3, 21.4R3, 22.1R2, 22.2R1 et suivantes de Junos OS.

Source : https://bit.ly/3U66DQK

Actualité

Ducktail : un nouveau malware PHP distribué sous la forme d'applications craquées !

L'équipe de recherche de Zscaler ThreatLabz a identifié une version PHP de 'Ducktail' Infostealer distribuée sous la forme d'un installateur d'application craqué pour une variété d'applications, y compris des jeux, des applications Microsoft Office, Telegram, et autres.

Selon les experts, Ducktail est actif depuis 2021 et pourrait être exploité par un groupe de menaces vietnamien. L'objectif principal de cette campagne d'attaque est de prendre le contrôle de comptes Facebook Business.

Les versions antérieures (observées par WithSecure Labs) étaient basées sur un binaire écrit en utilisant - NetCore avec Telegram comme canal C2 pour exfiltrer les données.

Dans ce cas, le programme d'installation malveillant est hébergé

sur un site Web d'hébergement de fichiers. En comparant avec les campagnes précédentes, les chercheurs affirment que des changements ont été apportés dans l'exécution du code malveillant. En outre, les acteurs de la menace sont passés à une version de script dans laquelle le code principal du voleur est un script PHP et non un binaire .Net.

" À son exécution, le faux programme d'installation fait apparaître une interface graphique 'Checking Application Compatibility' en avant-plan. En arrière-plan, il génère un fichier .tmp qui relance le programme d'installation avec le paramètre "/Silent", puis un autre fichier .tmp est généré", indiquent les chercheurs de Zscaler.

Les chercheurs affirment que le code du voleur est décrypté au moment de l'exécution dans la mémoire et effectue ensuite des opérations de vol et d'exfiltration de données.

Il récupère les informations du navigateur installé dans le système et extrait les informations stockées dans les cookies tout en ciblant les comptes Facebook Business.

En recherchant les liens Facebook Business Ads Manager, le code malveillant accède aux détails des comptes et des cycles de paiement. Puis il tente d'obtenir la liste des détails à partir des pages Facebook Business tels que 'montant dépensé', 'détails de la devise', 'mode de paiement', etc.

"La campagne de vol de Ducktail apporte continuellement des modifications ou des améliorations aux mécanismes de diffusion afin de voler une grande variété d'informations sensibles sur les utilisateurs et les systèmes, en ciblant les utilisateurs en général", ont déclaré les chercheurs.

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

Le ransomware BlackByte utilise un pilote légitime pour désactiver les produits de sécurité

Le groupe de ransomware BlackByte utilise actuellement une nouvelle technique appelée "Bring Your Own Driver", qui lui permet de contourner diverses mesures de sécurité.

Les récentes attaques attribuées à ce groupe impliquaient une version du pilote MSI Afterburner RTCore64.sys, qui est vulnérable à une faille d'élévation de privilèges et d'exécution de code repérée sous le nom de CVE-2019-16098.

L'exploitation de ce problème de sécurité a permis à BlackByte de désactiver des pilotes qui empêchent plusieurs produits de détection et de réponse (EDR) et antivirus de fonctionner normalement.

La méthode "Bring Your Own Vulnerable Driver" est efficace car les pilotes vulnérables sont signés avec un certificat valide et s'exécutent avec des privilèges élevés sur le système.

Deux exemples récents d'attaques BYOVD sont l'utilisation par Lazarus d'un pilote Dell défectueux et l'utilisation par des pirates inconnus d'un pilote/module anti-triche pour le jeu Genshin Impact. Selon les chercheurs de Sophos, le pilote graphique MSI utilisé abusivement offre des codes de contrôle d'E/S directement accessibles par les processus en mode utilisateur, ce qui viole les directives de sécurité de Microsoft sur l'accès à la mémoire du noyau. Cela permet aux attaquants de lire, écrire ou exécuter du code dans la mémoire du noyau sans utiliser de shellcode ou d'exploit.

En premier, BlackByte identifie la version du noyau pour sélectionner les bons offsets qui correspondent à l'ID du noyau. Ensuite, RTCore64.sys est déposé dans "AppData\Roaming" et crée un service en utilisant un nom codé en dur et un nom d'affichage aléatoire.

Les attaquants exploitent ensuite la vulnérabilité du pilote pour supprimer les routines de notification du noyau qui correspondent aux processus des outils de sécurité.

Les adresses de rappel récupérées sont utilisées pour dériver le nom du pilote correspondant et comparées à une liste de 1 000 pilotes ciblés qui prennent en charge la fonction des outils AV/EDR.

Toute correspondance trouvée à ce stade est supprimée en écrasant par des zéros l'élément qui contient l'adresse de la fonction de rappel, de sorte que le pilote ciblé est annulé.

Sophos met également en évidence plusieurs méthodes employées par BlackByte dans ces attaques pour échapper à l'analyse des chercheurs en sécurité, comme la recherche de signes d'un débogueur en cours d'exécution sur le système cible et sa fermeture.

Le malware BlackByte recherche également une liste de DLL d'accrochage utilisées par Avast, Sandboxie, Windows DbgHelp Library et Comodo Internet Security, et met fin à son exécution si elle est trouvée.

Les administrateurs système peuvent se protéger contre cette nouvelle astuce de contournement de la sécurité de BlackByte en ajoutant le pilote MSI en question à une liste de blocage active.

En outre, les administrateurs doivent surveiller tous les événements d'installation de pilotes et les examiner fréquemment pour trouver toute injection malveillante qui n'a pas de correspondance matérielle.

Source : *https://bit.ly/3DkCw1e*

Toyota signale une fuite de données après l'exposition d'une clé d'accès sur GitHub

Toyota Motor Corporation annonce que les données personnelles de ses clients pourraient avoir été exposées après qu'une clé d'accès ait été publiquement disponible sur GitHub pendant près de cinq ans.

Toyota T-Connect est l'application de connectivité officielle du constructeur automobile qui permet aux propriétaires de voitures Toyota de relier leur smartphone au système d'info-divertissement du véhicule pour les appels téléphoniques, la musique, la navigation, l'intégration des notifications, les données de conduite, l'état du moteur, la consommation de carburant, etc.

Toyota a découvert récemment qu'une partie du code source de cette application avait été publiée par erreur sur GitHub et contenait une clé d'accès au serveur de données qui stockait les adresses électroniques et les numéros de gestion des clients.

Cela a permis à un tiers non autorisé d'accéder aux détails de 296 019 clients entre décembre 2017 et le 15 septembre 2022, date à laquelle l'accès au référentiel GitHub a été restreint. Ensuite, les clés de base de données ont été changées ce qui empêche tout accès non autorisés.

Selon la société, les noms des clients, les données des cartes de crédit et les numéros de téléphone n'ont pas été compromis, car ils n'étaient pas stockés dans la base de données exposée.

Toyota a attribué la responsabilité de l'erreur à un sous-traitant de développement, mais a reconnu sa responsabilité dans la mauvaise gestion des données des clients et s'est excusé pour tout désagrément causé.

"À la suite d'une enquête menée par des experts en sécurité, bien que nous ne puissions pas confirmer l'accès par un tiers sur la base de l'historique d'accès au serveur de données où l'adresse e-mail du client et le numéro de gestion du client sont stockés, dans le même temps, nous ne pouvons pas le nier complètement.", explique Toyota.

Pour cette raison, il est conseillé à tous les utilisateurs de T-Connect qui se sont inscrits entre juillet 2017 et septembre 2022 d'être vigilants face aux escroqueries par hameçonnage et d'éviter d'ouvrir les pièces jointes des courriels provenant d'expéditeurs inconnus prétendant être de Toyota.

Ce type d'incident de sécurité résulte généralement de la négligence des développeurs, qui stockent les informations d'identification dans le code pour faciliter l'extraction des ressources, l'accès aux services et la mise à jour de la configuration tout en testant plusieurs itérations de l'application. Ces informations d'identification devraient être supprimées lorsque le logiciel est prêt à être déployé, mais malheureusement, comme le montre le cas de l'application T-Connect, ce n'est pas toujours le cas.

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

Les exploitants de Raspberry Robin vendent aux gangs de ransomware l'accès initial à des réseaux d'entreprise compromis

Armorblox Security a découvert une nouvelle campagne de phishing d'identifiants qui permet de contourner la sécurité de la messagerie de Google. La campagne est menée sur LinkedIn puisque les médias sociaux continuent d'être une bonne source de cibles pour les cybercriminels.

La campagne de phishing a ciblé 500 boîtes aux lettres d'employés d'une organisation nationale de voyages. L'e-mail a pour objet "Nous avons remarqué une activité inhabituelle" et prétend provenir de LinkedIn.

Cependant, les attaquants ont mal orthographié LinkedIn et le domaine a été créé le 6 mars.

La campagne de phishing n'a pas été détectée par les contrôles de sécurité des e-mails de Google après avoir passé les contrôles d'authentification via DMARC (Domain-based message authentication, reporting and conformance) et SFP (Sender Policy Framework).

Elle s'appuie sur l'usurpation d'identité, l'ingénierie sociale, des URL malveillantes et la reproduction de flux de travail existants.

Au troisième trimestre, LinkedIn est devenue la troisième marque la plus usurpée, précédée par DHL et Microsoft. Elle était pourtant en tête de liste au cours des deux trimestres précédents de l'année.

Les acteurs de la menace ont créé de faux comptes d'employés sur LinkedIn, qui couplent des photos de profil générées par l'IA avec du texte copié sur des utilisateurs légitimes.

LinkedIn a introduit trois nouvelles fonctionnalités pour se défendre contre les faux profils et les activités malveillantes sur la plateforme.

LinkedIn a commencé à montrer plus d'informations sur les comptes pour les vérifier, à faire une chasse active aux fausses IA et à avertir les utilisateurs contre les messages suspects.

Ces dernières années, les acteurs malveillants ont largement utilisé LinkedIn pour voler les informations d'identité des utilisateurs et attaquer les réseaux d'entreprise. Au lieu de se fier uniquement à la sécurité native des e-mails, Armorblox conseille d'ajouter une couche supplémentaire de sécurité de la messagerie. En outre, il convient de prêter attention aux indices d'ingénierie sociale et de mettre en place un système d'authentification multi facteur.

Source : *https://bit.ly/3SUt8am*

Bon à savoir

Les données des Honeypots révèlent les caractéristiques des attaques de robots contre RDP et SSH

Les honeypots RDP et SSH de Rapid7 ont collecté des données entre le 10 septembre 2021 et le 9 septembre 2022, dont l'examen a révélé des dizaines de millions de tentatives de connexion. Grâce à l'utilisation des honeypots RDP et SSH, ils ont enregistré 512 002 mots de passe différents et 215 894 adresses IP sources différentes. Le fichier rockyou2021.txt contient presque tous les mots de passe récupérés (99,997 %).

En 2009, Rockyou a été piraté. Les attaquants ont découvert 32 millions de comptes utilisateurs en clair et les ont pris. Une liste de 14 341 564 mots de passe, rendue publique par la suite, est devenue le fichier original rockyou.txt, qui a été distribué avec Kali Linux pour faciliter les tests de pénétration et est fréquemment utilisé dans les attaques par dictionnaire.
La liste originale de mots de passe a été élargie au cours des années suivantes et, par conséquent, la collection rockyou2021.txt contient désormais 8,4 milliards de mots de passe dans un fichier texte de 92 Go. Sur GitHub, ce fichier est librement accessible.
L'analyse par Rapid7 des mots de passe utilisés montre une forte préférence pour les mots de passe standard connus couramment utilisés. Les cinq principales tentatives de mot de passe RDP étaient ' ' (la chaîne vide), '123', 'password', '123qwe' et 'admin'. Les cinq principales tentatives de mot de passe SSH étaient '123456', 'nproc', 'test', 'qwerty' et 'password'. Ces mots de passe et tous les autres pourraient provenir de rockyou2021.
Cependant, rockyou2021 n'est en fait qu'une longue liste de mots. Elle exclut les chaînes de caractères arbitraires, mixtes ASCII et spéciaux.
La recherche de Rapid7 est arrivée à la conclusion que l'utilisation de chaînes aléatoires longues et fortes, telles que celles produites par les gestionnaires de mots de passe et peu susceptibles d'être trouvées dans les "dictionnaires", offrirait une très forte résistance aux attaques automatisées menées par des robots opportunistes.
Selon Rapid7, la longueur est encore plus importante que la complexité du mot de passe car les attaques par dictionnaires devront plus difficiles à mettre en œuvre pour chaque augmentation dans la longueur du mot de passe.
Toutefois, la principale conclusion de cette étude est que la prochaine génération d'attaques automatisées opportunistes contre RDP et SSH sera probablement vaincue si les entreprises et les particuliers s'entraînent à créer des mots de passe d'une longueur suffisante, contenant quelques caractères spéciaux.

Source : *https://bit.ly/3gXIe1H*

Evènements

Evènement du mois

Reduce data breaches : Best practice for web app security

31 Octobre 2022

Online

https://bit.ly/3FuSM2h

L'évolution de la technologie a abordé plusieurs avantages aux applications web, mais pour garantie leur sécurité est devenue plus critique que jamais. Le dernier rapport de Verizon sur les incidents de violation de données indique que les applications web sont devenues la première forme de violation. La question qui se pose est la suivante : comment savoir si les mesures prises pour protéger nos applications web et sécuriser les données sont suffisantes ?

Cette conférence abordera la mise en œuvre d'un processus et d'une méthodologie standardisés pour tester les applications Web de manière complète, reproductible et reconnue par l'industrie.

Evènement à venir

SECUREWORLD Seattle

09-10 Novembre 2022

Online

https://bit.ly/3gXwwEf

Depuis plus de 20 ans, les conférences SecureWorld connectent, informent et développent les leaders de la cybersécurité.

Cet évènement est une formation et une collaboration de haute qualité des professionnels de l'InfoSec, que ce soit virtuellement ou en personne.

Le participant peut obtenir de 6 à 12 crédits CPE grâce à plus de 20 éléments éducatifs, en apprenant des leaders du secteur reconnus au niveau national.

Il y'aura des discours-programmes, des discussions de groupe, des sessions en petits groupes et des opportunités de réseautage. Évaluation des solutions des fournisseurs et rencontre des sections locales des associations de sécurité.

Référence	ANPT-2022-BV-10
Titre	Bulletin de veille N°10
Date de version	31 Octobre 2022
Contact	ssi@anpt.dz