BULLETIN DE VEILLE N°04

ANPT-2023-BV-04

« L'un des tests du leadership est la capacité de reconnaître un problème avant qu'il ne devienne une urgence. »
- Arnold H. Glasow-

Avril 2023

Alertes de sécurité

Apple

Apple déploie des correctifs pour les anciennes versions d'iOS et de macOS

11 Avril 2023

Apple a informé ses clients que iOS et iPadOS 16.4.1 et macOS Ventura 13.3.1 corrigent CVE-2023-28206 et CVE-2023-28205, deux vulnérabilités zero-day.
CVE-2023-28206 concerne le composant IOSurfaceAccelerator et peut permettre à une application malveillante d'exécuter du code avec les privilèges du noyau. CVE-2023-28205 affecte WebKit et peut être exploité en attirant l'utilisateur ciblé vers un site web malveillant.
Apple a publié iOS et iPadOS 15.7.5 pour corriger les failles des iPhone 6s, iPhone 7, iPhone SE et des anciens iPads. Il a également publié les mises à jour de macOS Monterey et Big Sur pour corriger les vulnérabilités CVE-2023-28206.
Les failles de sécurité ont probablement été exploitées par des fournisseurs de logiciels espions commerciaux.
La société, qui suit plus de 30 fournisseurs de logiciels espions, a décrit les vulnérabilités de Chrome, de WebKit et des pilotes de noyau exploitées dans des attaques sophistiquées dont l'objectif est de pirater les appareils des personnes ciblées.

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

Android

Android corrige des vulnérabilités critiques d'exécution de code à distance

5 Avril 2023

Le bulletin de sécurité Android pour avril 2023 décrit 26 vulnérabilités résolues dans les composants Framework et System dans le cadre du niveau de correctif de sécurité 2023-04-01. La plupart d'entre elles sont des failles de haute gravité conduisant à l'élévation des privilèges (EoP) ou à la divulgation d'informations.

Deux des 16 problèmes abordés dans System, cependant, sont des bogues RCE de gravité critique, suivis comme CVE-2023-21085 et CVE-2023-21096.

La deuxième partie du correctif de sécurité 2023-04-05 comprend des correctifs pour 40 vulnérabilités dans les composants kernel, Arm, Imagination Technologies, MediaTek, Unisoc et Qualcomm, quatre de ces problèmes sont considérés comme étant de "gravité critique".

Google n'a pas publié de bulletin de sécurité Pixel le jour même de l'annonce des correctifs Android. Cependant, les utilisateurs de Pixel ont reçu une mise à jour en mars, bien qu'ils aient dû attendre quelques jours de plus avant qu'elle n'arrive.

Source : *https://bit.ly/424s0pu*

Sophos

Sophos corrige une vulnérabilité critique d'exécution de code dans le Web Security Appliance

07 Avril 2023

Sophos a annoncé des mises à jour de sécurité automatique qui résolvent plusieurs vulnérabilités dans Sophos Web Appliance.

Sophos Web Appliance permet aux administrateurs de mettre en place des politiques d'accès web.

Le problème critique, répertorié sous le nom de CVE-2023-1671 (score CVSS de 9.8), a été identifié dans le gestionnaire de la page d'avertissement de l'appliance et il pourrait être exploité sans authentification.

L'entreprise de cybersécurité a résolu la faille avec la publication de Sophos Web Appliance 4.3.10.4, qui corrige également la faille d'injection de commande CVE-2022-4934 (score CVSS de 7.2) et la faille de type type cross-site scripting (XSS) CVE-2020-36692 (gravité moyenne).

Les correctifs pour toutes les vulnérabilités sont fournis aux utilisateurs de Sophos Web Appliance via des mises à jour automatiques. Sophos recommande de placer l'appliance derrière un pare-feu et de bloquer l'accès à Internet.

Sophos Web Appliance devrait arriver en fin de vie le 20 juillet 2023. Sophos recommande aux clients de Web Appliance de migrer vers Sophos Firewall.

Source : *https://bit.ly/3Vie2OG*

Actualité

Des employés de Samsung ont involontairement divulgué des données secrètes de l'entreprise en utilisant ChatGPT

Des documents internes de Samsung, tels que des notes de conférence et le code source, ont été partagés avec le populaire service de chatbot ChatGPT.

Les ingénieurs de Samsung ont utilisé ChatGPT pour évaluer le code source de l'entreprise, ils ont demandé au chatbot d'optimiser les séquences de test pour identifier les défauts dans les puces qu'ils étaient en train de concevoir. Selon le site web Techradar, en un peu moins d'un mois, l'entreprise a subi trois fuites de données causées par ses employés qui ont divulgué des informations sensibles via ChatGPT.

"Dans un autre cas, un employé a utilisé ChatGPT pour convertir des notes de réunion en une présentation, dont le contenu n'était manifestement pas quelque chose que Samsung aurait voulu que des tiers externes connaissent", a rapporté TechRadar.

L'entreprise informatique internationale a pris la décision de commencer à créer sa propre IA pour un usage interne.

Samsung Electronics met en garde ses employés contre les risques potentiels liés à l'utilisation de ChatGPT, expliquant qu'il n'y a aucun moyen d'empêcher la fuite des données fournies au service de chatbot d'OpenAI.

Au début de ce mois, l'autorité italienne de protection des données, Garante Privacy, a temporairement interdit ChatGPT en raison de la collecte non autorisée d'informations personnelles et de l'absence de méthodes permettant de confirmer l'âge des mineurs.

L'autorité a attiré l'attention sur le fait qu'OpenAI n'informe pas les utilisateurs qu'elle collecte leurs données.

Le communiqué affirme qu'il n'existe aucune justification légale à la collecte et au traitement intensifs des données personnelles utilisées pour "entraîner" les algorithmes de la plateforme.

Source : *https://bit.ly/3Hw9CON*

Des pirates ciblent les serveurs de sauvegarde vulnérables de Veeam exposés en ligne

Les serveurs de sauvegarde Veeam sont la cible d'au moins un groupe d'acteurs de la menace connus pour travailler avec plusieurs gangs de ransomware de premier plan.

Des activités malveillantes et des outils faisant écho aux attaques FIN7 ont été observés dans des intrusions depuis le 28 mars, moins d'une semaine après la mise à disposition d'un exploit pour une vulnérabilité de haute sévérité dans le logiciel Veeam Backup and Replication (VBR).

Repérée sous le nom de CVE-2023-27532, le problème de sécurité expose les informations d'identification chiffrées stockées dans la configuration de VBR à des utilisateurs non authentifiés dans l'infrastructure de sauvegarde. Ces informations peuvent être utilisées pour accéder aux hôtes de l'infrastructure de sauvegarde.

Lors d'un exercice de chasse aux menaces utilisant les données télémétriques de WithSecure Endpoint Detection and Response (EDR), les chercheurs ont remarqué que certains serveurs Veeam généraient des alertes suspectes (par exemple, sqlservr.exe générant cmd.exe et téléchargeant des scripts PowerShell).

Un examen plus approfondi a montré que l'acteur de la menace a d'abord exécuté le script PowerShell PowerTrash, vu dans des attaques antérieures attribuées à FIN7, qui incluait une charge utile - la porte dérobée DiceLoader/Lizar, à exécuter sur la machine compromise.

DiceLoader, également repéré sous le nom de Tirion, a également été lié aux activités malveillantes de FIN7 par le passé. Il convient de noter que des incidents plus récents attribués à ce gang ont utilisé une porte dérobée différente que les chercheurs de Mandiant appellent PowerPlant.

WithSecure souligne que les noms des scripts PowerShell (icsnd16_64refl.ps1, icbt11801_64refl.ps1) observés dans les attaques suivent la convention de dénomination précédemment signalée pour les fichiers FIN7.

Un script PowerShell (host_ip.ps1) pour la résolution des adresses IP en noms d'hôtes et un script personnalisé utilisé pour la reconnaissance dans la phase de mouvement latéral de l'attaque sont également connus pour faire partie de la boîte à outils de FIN7.

M. Singh a indiqué qu'il avait également observé d'autres recoupements techniques avec des rapports antérieurs sur des activités attribuées à FIN7. Il s'agit par exemple de schémas d'exécution de la ligne de commande et de conventions de dénomination des fichiers.

Une fois qu'ils ont eu accès à l'hôte, les pirates ont utilisé leur logiciel malveillant, diverses commandes et des scripts personnalisés pour collecter des informations sur le système et le réseau, ainsi que des informations d'identification à partir de la base de données de sauvegarde Veeam.

L'acteur de la menace a également tenté un mouvement latéral en utilisant des informations d'identification volées, en testant leur accès avec des invocations WMI et des commandes 'net share'.

WithSecure recommande aux organisations qui utilisent le logiciel de sauvegarde et de réplication Veeam de tenir compte des informations fournies et de les utiliser pour rechercher des signes de compromission sur leur réseau.

Même si la méthode exacte pour invoquer les commandes shell initiales reste inconnue et que la preuve de l'exploitation de CVE-2023-27532 n'est pas claire, les entreprises devraient donner la priorité à la correction de la vulnérabilité car d'autres acteurs de la menace pourraient essayer de l'exploiter.

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

Bon à savoir

Des pirates cachent des portes dérobées derrière des archives auto-extractibles malveillantes

Des acteurs de la menace ajoutent des fonctionnalités malveillantes aux archives auto-extractibles WinRAR (SFX) afin d'installer des portes dérobées persistantes dans les systèmes cibles sans qu'elles soient détectées. Ces fichiers SFX contiennent des fichiers leurres qui peuvent lancer PowerShell, l'invite de commande et le gestionnaire de tâches avec les privilèges du système.

Selon les chercheurs de CrowdStrike, les acteurs de la menace commencent par installer sur le système ciblé un fichier SFX protégé par un mot de passe, créé à l'aide de WinRAR ou de 7-Zip.

- Ils accèdent au système à l'aide d'informations d'identification compromises et tentent d'abuser d'une application d'accessibilité légitime de Windows appelée Utility Manager (utilman[.]exe).
- L'application est ensuite paramétrée pour configurer un débogueur IFEO (Image File Execution Options) dans le registre Windows pour un programme spécifique. Elle démarre automatiquement le débogueur à chaque fois que le programme est lancé.
- L'utilman[.]exe déclenche le fichier SFX qui contient un fichier texte qui est conçu pour abuser des options de configuration de WinRAR afin d'exécuter PowerShell, d'ajouter plusieurs commandes et de créer une archive SFX pour ouvrir une porte dérobée sur le système.

Même si les utilisateurs cibles ne disposent pas de logiciels de décompression tels que WinRAR ou 7-Zip, les fichiers SFX se décompressent de manière transparente et affichent le contenu des fichiers sans ces logiciels.

Pour éviter de telles attaques, il est conseillé aux utilisateurs de prêter une attention particulière aux archives SFX et d'utiliser un logiciel de désarchivage approprié ou d'autres outils pour vérifier le contenu de l'archive. En outre, il est recommandé d'analyser les archives SFX pour y déceler d'éventuelles fonctionnalités cachées.

Source : *https://bit.ly/3LL1iNl*

Evènements

Evènement du mois

Compétences générales recherchées par les employeurs en cybersécurité

30 Avril 2023

Online

https://bit.ly/3VmhdVE

L'événement SafeTeensOnline consiste sur le développement des compétences générales demandées par les employeurs dans le domaine de la cybersécurité constitue une plateforme unique pour les jeunes qui peuvent ainsi bénéficier des connaissances précieuses de M. Leber et d'autres experts de l'industrie.

En participant à des exercices pratiques et en écoutant des professionnels de premier plan, les participants peuvent développer les compétences non techniques qui sont essentielles pour réussir dans le domaine de la cybersécurité.sécurité.

Evènement à venir

Étendre la portée du renseignement sur les menaces : La nécessité d'une défense collective

16 Mai 2023

Online

https://bit.ly/41XjskD

Dans le secteur de la santé, il est plus que jamais essentiel que les bonnes informations sur les menaces parviennent aux bonnes personnes au bon moment. Alors que les équipes de sécurité sont inondées de flux de menaces, il est difficile de donner un sens à ce flot d'informations, et encore plus difficile de partager des informations et de réagir rapidement à travers les organisations distribuées. Rejoignez les experts de Health-ISAC et de Cyware pour une discussion interactive et découvrez comment vos pairs étendent la portée des renseignements sur les menaces grâce à la collaboration et à l'automatisation, afin d'obtenir les avantages d'une défense collective.

Référence	ANPT-2023-BV-04
Titre	Bulletin de veille N°04
Date de version	30 Avril 2023
Contact	ssi@anpt.dz