BULLETIN DE VEILLE N°06

ANPT-2023-BV-06

"It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."
- Stephane Nappo -

Juin 2023

Alertes de sécurité

Chrome 114

Google corrige la troisième faille zéro de Chrome en 2023

07 Juin 2023

Google a publié une mise à jour de sécurité Chrome 114 qui corrige la troisième vulnérabilité Zero-Day trouvée dans le navigateur web en 2023.

La dernière version de Chrome corrige deux failles, dont la CVE-2023-3079, un problème de confusion de type affectant le moteur JavaScript V8.

La vulnérabilité a été exploitée dans la nature probablement par un éditeur de logiciels espions commerciaux, mais n'a pas partagé d'informations sur les attaques.

Dans de nombreux cas, les éditeurs de logiciels espions intègrent les vulnérabilités de Chrome dans des chaînes d'exploitation complexes conçues pour cibler les appareils Android.

Source : *https://bit.ly/3p82EJN*

La mise à jour Chrome 114 corrige une vulnérabilité critique

14 Juin 2023

Une nouvelle version du navigateur Chrome 114 arrive environ une semaine après que Google a publié une mise à jour d'urgence de Chrome pour corriger une vulnérabilité zero-day.

Cette nouvelle mise à jour résout cinq vulnérabilités, dont quatre bogues critiques et de haute sévérité signalés par des chercheurs externes.

Le plus important de ces problèmes est CVE-2023-3214, une faille critique de type "use-after-free" dans les paiements Autofill. Le problème a été signalé par Rong Jian de VRI.

Les failles de type "use-after-free" sont un type de bogues de corruption de mémoire qui se produisent lorsqu'un pointeur n'est pas effacé après qu'une allocation de mémoire a été libérée.

L'exploitation réussie des vulnérabilités "use-after-free" peut conduire à une évasion de la Sandbox, si l'attaquant peut cibler un processus privilégié de Chrome ou une faille dans le système d'exploitation sous-jacent.

La mise à jour résout deux autres problèmes de type "use-after-free", tous deux classés dans la catégorie "haute gravité" : CVE-2023-3215, qui affecte WebRTC, et CVE-2023-3217, qui affecte WebXR.

La quatrième faille signalée en externe et résolue avec cette version du navigateur est un problème de confusion de type dans le moteur JavaScript V8.

Google ne fait aucune mention de l'exploitation de ces vulnérabilités dans le cadre d'attaques.

La dernière version de Chrome est désormais disponible sous la forme de la version 14.0.5735.133 pour macOS et Linux, et sous la forme des versions 114.0.5735.133/134 pour Windows.

Source : *https://bit.ly/3Xcy3HA*

Android

La mise à jour de sécurité d'Android de juin 2023 corrige une vulnérabilité exploitée par le GPU Arm

08 Juin 2023

Les mises à jour de sécurité annoncées par Google pour le système d'exploitation Android corrigent plus de 50 vulnérabilités, dont une faille du GPU Arm Mali exploitée par des éditeurs de logiciels espions.
Identifié sous le nom de CVE-2022-22706, le bogue exploité est un problème de pilote de noyau qu'Arm a corrigé en janvier 2022, mais qui avait été ciblé dans des attaques avant cela, a rapporté Google en mars 2023.
Malgré l'exploitation connue, Google et les autres fournisseurs d'Android ont mis plus d'un an à intégrer les correctifs pour CVE-2022-22706 dans leurs mises à jour logicielles.
La mise à jour Android de juin 2023 est divisée en deux parties.
La première partie, qui arrive sur les appareils sous la forme du niveau de correctif de sécurité 2023-06-01, résout 10 vulnérabilités dans le composant Framework et 13 bugs dans le composant System.

Trois de ces problèmes sont des failles d'exécution de code à distance (RCE) de gravité critique. Elles sont répertoriées sous les noms de CVE-2023-21127, CVE-2023-21108 et CVE-2023-21130.
Le plus grave de ces problèmes est une vulnérabilité de sécurité critique dans le composant Système qui pourrait conduire à l'exécution de code à distance via Bluetooth, si la prise en charge HFP est activée, sans privilèges d'exécution supplémentaires nécessaires. L'interaction de l'utilisateur n'est pas nécessaire pour l'exploitation.
Classées dans la catégorie " gravité élevée ", les 20 autres vulnérabilités entraînent une escalade des privilèges, une divulgation d'informations ou un déni de service (DoS).
Arrivée sur les appareils sous la forme du correctif de sécurité 2023-06-05, la deuxième partie de la mise à jour 2023 d'Android résout 33 failles dans les composants Arm (3 vulnérabilités), Imagination Technologies (2), Unisoc (4), Widevine DRM (2) et Qualcomm (22).

Source : *https://bit.ly/3N7bZte*

Zyxel

Zyxel invite ses clients à mettre à jour les pare-feux contre les vulnérabilités exploitées

05 Juin 2023

Zyxel invite ses clients à mettre à jour les pare-feux ATP, USG Flex, VPN et ZyWALL/USG afin d'empêcher l'exploitation des récentes vulnérabilités.

Identifiées comme CVE-2023-28771, CVE-2023-33009 et CVE-2023-33010, ces vulnérabilités peuvent conduire à l'exécution de commandes du système d'exploitation, à l'exécution de code à distance (RCE) et à un déni de service (DoS).

Le fabricant souligne que les notifications push via les interfaces graphiques Web et les mises à jour programmées du micrologiciel pour les appareils basés sur le cloud.

La société conseille également aux clients de désactiver les services HTTP/HTTPS du réseau étendu s'ils ne sont pas utilisés, d'activer le contrôle des politiques et de n'autoriser l'accès qu'à partir d'IP de confiance, d'activer le filtrage géoIP et de désactiver les ports UDP 500 et 4500 s'ils ne sont pas utilisés.

Pour identifier les infections potentielles par des logiciels malveillants, les clients doivent rechercher des symptômes tels que des appareils qui ne répondent pas, des interfaces Web ou des interfaces de gestion SSH inaccessibles, des interruptions du réseau et des connexions VPN déconnectées.

Source : *https://bit.ly/42d4mXB*

Cisco

Cisco corrige une vulnérabilité critique dans les solutions de collaboration d'entreprise

08 Juin 2023

Cisco a annoncé des correctifs pour une vulnérabilité critique dans ses solutions de collaboration et de communication vidéo d'entreprise Expressway series et TelePresence Video Communication Server (VCS).

Identifiée comme CVE-2023-20105 (score CVSS de 9,6), la vulnérabilité permet à un administrateur disposant de droits de "lecture seule" d'élever ses privilèges à "lecture-écriture".

Les déploiements de la série Cisco Expressway et TelePresence VCS qui ont accordé un accès CLI à un administrateur en lecture seule sont également vulnérables à la CVE-2023-20192, une vulnérabilité de haute sévérité conduisant également à une escalade des privilèges. Selon Cisco, l'accès au CLI est désactivé par défaut pour les utilisateurs en lecture seule.

La version 14.2.1 de la série Expressway et du TelePresence VCS contient des correctifs pour CVE-2023-20105, tandis que la version 14.3.0 corrige CVE-2023-20192.

Cisco a également annoncé des correctifs pour des bogues de déni de service (DoS) de haute sévérité dans le service Unified Communications Manager IM & Presence et les appliances de la série Firepower 2100, ainsi qu'une faille d'exécution de code de haute sévérité dans le logiciel AnyConnect Secure Mobility Client et Secure Client pour Windows.

Cisco a également publié des correctifs pour deux vulnérabilités de gravité moyenne, à savoir un bogue DoS dans Unified Communications Manager et Unified Communications Manager Session Management Edition et un problème d'escalade des privilèges dans Secure Workload.

Source : *https://bit.ly/3qU4xtS*

Adobe

Patch Tuesday : des failles critiques dans le logiciel Adobe Commerce

13 Juin 2023

Dans le cadre de son lot de mises à jour Patch Tuesday, Adobe a documenté au moins 12 problèmes de sécurité dans le produit largement déployé Adobe Commerce (anciennement Magento) et a averti qu'une exploitation réussie pouvait conduire à l'exécution de code arbitraire, au contournement des fonctions de sécurité et à la lecture arbitraire du système de fichiers.

Un bulletin de sécurité critique d'Adobe indique que le produit Magento Open Source est également vulnérable aux problèmes documentés.

La société a également fourni des correctifs pour quatre bogues documentés qui pourraient conduire à des exploits ciblant le logiciel Adobe Experience Manager.

Le déploiement du Patch Tuesday comprend également des correctifs pour une faille critique dans Adobe Animate qui pourrait causer des problèmes d'exécution de code dans le contexte de l'utilisateur actuel.

Les mises à jour couvrent également un bogue majeur dans Adobe Substance 3D Designer qui expose également les utilisateurs à des risques d'exécution de code.

Adobe a déclaré qu'il n'avait connaissance d'aucun exploit dans la nature pour l'un des problèmes abordés dans les mises à jour de ce mois.

Source : *https://bit.ly/3NBo6A4*

Actualité

Plus de 100 000 identifiants de comptes ChatGPT volés vendus sur les places de marché du Dark Web

Plus de 100 000 identifiants de comptes ChatGPT d'OpenAI compromis se sont retrouvés sur des places de marché illicites du dark web entre juin 2022 et mai 2023, l'Inde représentant à elle seule 12 632 identifiants volés.

Les autres pays ayant le plus grand nombre d'identifiants ChatGPT compromis sont le Pakistan, le Brésil, le Vietnam, l'Égypte, les États-Unis, la France, le Maroc, l'Indonésie et le Bangladesh.

Une analyse plus approfondie a révélé que la majorité des journaux contenant des comptes ChatGPT ont été violés par le célèbre voleur d'informations Raccoon, suivi par Vidar et RedLine.

Les voleurs d'informations sont devenus populaires parmi les cybercriminels en raison de leur capacité à détourner les mots de passe, les cookies, les cartes de crédit et d'autres informations des navigateurs, ainsi que les extensions de portefeuilles de crypto-monnaies.

"Les journaux contenant des informations compromises récoltées par les voleurs d'informations sont activement échangés sur les places de marché du dark web", a déclaré le Group-IB.

Des informations supplémentaires sur les journaux disponibles sur ces marchés comprennent les listes de domaines trouvés dans le journal ainsi que les informations sur l'adresse IP de l'hôte compromis.

Généralement proposés sur la base d'un modèle de tarification par abonnement, ils ont non seulement abaissé la barre de la cybercriminalité, mais servent également de canal pour lancer des attaques ultérieures à l'aide des informations d'identification siphonnées.

Pour limiter ces risques, il est recommandé aux utilisateurs de suivre des pratiques d'hygiène appropriées en matière de mots de passe et de sécuriser leurs comptes avec une authentification à deux facteurs (2FA) afin de prévenir les attaques de prise de contrôle de compte.

Ce développement intervient dans le cadre d'une campagne de logiciels malveillants qui utilise de fausses pages web et des contenus pour adultes pour diffuser un cheval de Troie d'accès à distance et un voleur d'informations appelé DCRat (ou DarkCrystal RAT), une version modifiée d'AsyncRAT.

Dans les cas observés, les victimes ont été incitées à télécharger des fichiers ZIP contenant un chargeur VBScript qui est exécuté manuellement.

Elle fait également suite à la découverte d'une nouvelle variante VBScript d'un logiciel malveillant appelé GuLoader (alias CloudEyE) qui utilise des leurres sur le thème des impôts pour lancer des scripts PowerShell capables de récupérer et d'injecter le RAT Remcos dans un processus Windows légitime.

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

Des pirates infectent des serveurs SSH Linux avec le logiciel malveillant du botnet Tsunami

Un acteur inconnu procède à des forçages bruts sur des serveurs Linux SSH afin d'installer un large éventail de logiciels malveillants.

L'AhnLab Security Emergency Response Center (ASEC) a récemment découvert une campagne de ce type, qui piratait des serveurs Linux pour lancer des attaques DDoS et miner de la crypto-monnaie Monero.

Les attaquants ont scanné l'Internet à la recherche de serveurs Linux SSH exposés publiquement, puis ont forcé des paires de noms d'utilisateur et de mots de passe pour se connecter au serveur.

Une fois qu'ils ont pris pied sur le point d'accès en tant qu'utilisateur administrateur, ils ont exécuté une commande pour récupérer et exécuter un ensemble de logiciels malveillants via un script Bash.

L'ASEC a observé que les intrus ont également généré une nouvelle paire de clés SSH publiques et privées pour le serveur violé afin de maintenir l'accès même si le mot de passe de l'utilisateur a été modifié.

Les logiciels malveillants téléchargés sur les hôtes compromis comprennent des botnets DDoS, ShellBot, des nettoyeurs de journaux, des mineurs de crypto-monnaie XMRig (Monero) et des outils d'escalade des privilèges.

En commençant par ShellBot, ce bot DDoS basé sur Pearl utilise le protocole IRC pour communiquer. Il prend en charge le balayage de ports, les attaques par inondation UDP, TCP et HTTP et peut également mettre en place un shell inversé.

L'autre logiciel malveillant de réseau de zombies DDoS observé dans ces attaques est Tsunami, qui utilise également le protocole IRC pour communiquer.

La version particulière observée par l'ASEC est "Ziggy", une variante de Kaiten. Tsunami persiste entre les redémarrages en s'inscrivant lui-même dans "/etc/rc.local" et utilise les noms de processus typiques du système pour se cacher.

Tsunami prend également en charge un vaste ensemble de commandes de contrôle à distance, y compris l'exécution de commandes shell, les shells inversés, la collecte d'informations système, la mise à jour et le téléchargement de charges utiles supplémentaires à partir d'une source externe.

Viennent ensuite MIG Logcleaner v2.0 et Shadow Log Cleaner, deux outils utilisés pour effacer les preuves d'intrusion sur les ordinateurs compromis, de sorte que les victimes ont moins de chances de se rendre compte rapidement de l'infection.

Ces outils prennent en charge des arguments de commande spécifiques qui permettent aux opérateurs de supprimer des

journaux, de modifier des journaux existants ou d'ajouter de nouveaux journaux au système.

Le logiciel malveillant d'escalade des privilèges utilisé dans ces attaques est un fichier ELF (Executable and Linkable Format) qui élève les privilèges de l'attaquant à ceux d'un utilisateur root.

Enfin, les auteurs de la menace activent un mineur de monnaie XMRig pour détourner les ressources informatiques du serveur afin de miner du Monero sur un pool spécifié.

Pour se défendre contre ces attaques, les utilisateurs de Linux devraient utiliser des mots de passe de compte forts ou, pour une meilleure sécurité, exiger des clés SSH pour se connecter au serveur SSH.

En outre, il convient de désactiver la connexion root via SSH, de limiter la plage d'adresses IP autorisées à accéder au serveur et de remplacer le port SSH par défaut par un port atypique que les robots et les scripts d'infection ne verront pas.

Source : *https://bit.ly/3Pmt6tG*

Les clients de MOVEit sont invités à corriger une troisième vulnérabilité critique

Progress Software invite les clients de MOVEit à appliquer des correctifs à une troisième vulnérabilité critique du logiciel de transfert de fichiers en moins d'un mois.

Identifiée comme CVE-2023-35708, la dernière vulnérabilité est décrite comme une faille d'injection SQL qui pourrait permettre à un attaquant non authentifié d'élever ses privilèges et d'accéder au contenu de la base de données de MOVEit Transfer.

La vulnérabilité concerne les versions de MOVEit Transfer antérieures à 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7) et 2023.0.3 (15.0.3).

Le code de preuve de concept (PoC) ciblant le bogue a été publié le 15 juin, ce qui a suscité une réaction rapide de Progress, qui note que le bogue a été rendu public "d'une manière qui ne respecte pas les normes industrielles normales".

CVE-2023-35708 est la troisième faille critique d'injection SQL que Progress corrige dans ses produits MOVEit en trois semaines environ, après la divulgation d'une vulnérabilité zero-day le 31 mai et la correction d'une deuxième faille critique une semaine plus tard.

Le premier problème, CVE-2023-34362, a commencé à être largement exploité à la fin du mois de mai, mais les chercheurs en sécurité ont trouvé des preuves suggérant que l'exploitation pourrait avoir commencé il y a deux ans.

Plus de 100 organisations ont été touchées par des attaques ciblant le zero-day MOVEit, la récente campagne étant attribuée au gang du ransomware Cl0p, qui a commencé à nommer publiquement certaines des victimes.

Parmi les victimes connues à ce jour figurent le ministère américain de l'énergie, le bureau des véhicules motorisés de Louisiane, le ministère des transports de l'Oregon, le gouvernement de la Nouvelle-Écosse, British Airways, British Broadcasting Company, Aer Lingus, la chaîne de pharmacies Boots au Royaume-Uni, l'université de Rochester, le ministère de l'innovation et de la technologie de l'Illinois (DoIT) et le ministère de l'éducation du Minnesota (MDE).

Les victimes se trouvent en Autriche, en France, en Allemagne, au Luxembourg, aux Pays-Bas, en Suisse, au Royaume-Uni et aux États-Unis. Malwarebytes note que la plupart des victimes se trouvent aux États-Unis.

Le second problème, CVE-2023-35036, a été révélé le 9 juin, mais ne semble pas avoir été exploité dans la nature. Progress indique qu'il n'a aucune preuve que le problème CVE-2023-35708 ait été exploité, mais invite ses clients à appliquer les derniers correctifs dès que possible.

Pour empêcher tout accès non autorisé à l'environnement MOVEit Transfer, les clients doivent désactiver le trafic HTTP et HTTPS - en autorisant uniquement l'accès à l'hôte local - appliquer les correctifs disponibles (le correctif du 15 juin résout également les vulnérabilités précédentes), puis réactiver le trafic HTTP et HTTPS.

Source : *https://bit.ly/3JMFPT9*

Bon à savoir

Presque toutes les organisations ont subi une cyberattaque, selon Sophos

Une étude menée par Sophos révèle que les entreprises ont du mal à faire face à la vague incessante d'activités malveillantes. Au cours de l'année écoulée, 94 % des entreprises ont subi une forme ou une autre de cyberattaque. Les statistiques ci-dessous sont issues d'une enquête menée en janvier et février auprès de 3 000 responsables de la cybersécurité et de l'informatique dans 14 pays.

- Pour 41 % des organisations, l'exfiltration de données reste la principale préoccupation en matière de sécurité pour 2023, suivie par le phishing (40 %), les attaques par ransomware (35 %) et d'autres.
- 23 % des répondants ont déclaré avoir subi une attaque d'un adversaire actif en 2022. Les adversaires actifs sont des acteurs de la menace qui adaptent leurs TTP sur place en réponse aux technologies de sécurité et aux défenseurs.
- Les mauvaises configurations des contrôles de sécurité sont le risque de sécurité perçu le plus largement signalé, avec 27,4 % des organisations l'incluant dans leurs trois principaux risques de sécurité.
- Viennent ensuite les vulnérabilités de type "zero day" (26,8 %), la pénurie d'experts ou de compétences internes en cybersécurité (24,7 %) et le vol d'informations d'identification et d'accès (24 %).

Sophos recommande une approche en trois étapes pour remédier à la situation actuelle :

- Mettre en place un processus de réponse aux incidents plus évolutif qui accélère le temps de réponse.
- Utiliser des défenses adaptatives pour retarder les adversaires.
- Créer un cercle vertueux qui renforce la protection et réduit les coûts.

Les organisations devraient rapidement identifier les lacunes en matière de sécurité, évaluer leurs capacités et mettre en place une défense de cybersécurité appropriée pour faire face à ces menaces en plein essor.

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

Evènements

Evènement du mois

DevSecCon24

27 Juin 2023

Online

https://bit.ly/43W0G1k

24 heures d'action DevSecOps non-stop à DevSecCon24. Cet événement virtuel gratuit rassemble des experts et des praticiens des communautés DevOps, développement et sécurité pour une journée complète d'apprentissage, de réseautage et de collaboration.

Le but de cet évenement est de découvrir et définir les meilleures pratiques, les processus et les outils qui rendent les logiciels sécurisés possibles.

Evènement à venir

Programme de certificat en cybersécurité

17 Juillet 2023

Online

https://bit.ly/3XxEPYv

Formation à la cybersécurité destinée à combler le fossé entre les professionnels en quête d'une carrière et les employeurs désireux d'embaucher.

Cette formation a le but d'améliorer les compétences en cybernétique et d'apprendre des renseignements sur le nouveau programme de certificat en cybersécurité. Financé par une subvention du National Centers of Academic Excellence in Cybersecurity (situé au sein de la National Security Agency), les cours seront proposés à 100 % en ligne et comprendront des laboratoires d'apprentissage pratiques.

Référence	ANPT-2023-BV-06
Titre	Bulletin de veille N°06
Date de version	27 Juin 2023
Contact	ssi@anpt.dz