BULLETIN DE VEILLE N°02

ANPT-2023-BV-02

"If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you."
— Stephane Nappo --

Février 2023

Alertes de sécurité

Apple

Apple met à jour ses avis alors qu'une entreprise de sécurité divulgue une nouvelle classe de vulnérabilités

21 Février 2023

Apple a mis à jour plusieurs de ses récents avis de sécurité pour ajouter de nouvelles vulnérabilités à iOS et macOS, y compris celles appartenant à une nouvelle classe de bogues.

Les avis concernant iOS 16.3 et macOS Ventura 13.2 ont été mis à jour pour ajouter trois vulnérabilités. L'une d'entre elles est la CVE-2023-23520, une condition de course affectant le composant " crash reporter ", qui peut permettre à un attaquant de lire des fichiers arbitraires en tant que root.

Les deux autres failles de sécurité (CVE-2023-23530 et CVE-2023-23531) ont un impact sur le composant "foundation" des systèmes d'exploitation d'Apple et peuvent permettre à un attaquant d'exécuter du code arbitraire hors de sa sandbox ou avec certains privilèges élevés, elles ont aussi ouvert un énorme éventail de vulnérabilités potentielles que des chercheurs étudient actuellement.

Ces failles font partie d'une nouvelle classe de bugs qui peuvent permettre aux attaquants de contourner la signature de code sur les systèmes macOS et iOS.

Apple a pris des mesures pour empêcher l'exploitation, mais les chercheurs de Trellix ont découvert que les mesures d'atténuation du fournisseur pouvaient être contournées.

Apple a mis à jour ses avis de février pour ajouter une vulnérabilité de déni de service (DoS) signalée par un chercheur de Google.

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

Fortinet

Fortinet clarifie l'exploitation de la vulnérabilité FortiNAC

27 Février 2023

Fortinet a apporté des clarifications importantes suite à ce que la société a décrit comme des " rapports sensationnels " concernant de récentes tentatives d'exploitation d'une vulnérabilité dans sa solution de contrôle d'accès au réseau (NAC) FortiNAC.

La vulnérabilité, connue sous le nom de CVE-2022-39952, peut être exploitée par un attaquant distant et non authentifié pour une exécution de code arbitraire. Le problème a été découvert en interne par Fortinet.

Des correctifs pour la faille ont été annoncés le 16 février, et des détails techniques ainsi qu'un exploit de type "proof-of-concept" (PoC) ont été rendus publics par une société de cybersécurité le 21 février.

Le même jour, l'organisation de cybersécurité Shadowserver a commencé à voir des tentatives d'exploitation provenant de plusieurs adresses IP. Le lendemain, la société de renseignement sur les menaces GreyNoise a indiqué avoir constaté une large exploitation de CVE-2022-39952 à partir de deux adresses IP. Par contre, la société de sécurité Cronup, basée au Chili, a indiqué avoir constaté une "exploitation massive" provenant de 10 adresses IP.

L'impact réel de l'exploitation de CVE-2022-39952 reste à voir. Cependant, il est important que les utilisateurs de FortiNAC n'ignorent pas la menace potentielle, car des acteurs sophistiqués de la menace sont connus pour cibler les produits Fortinet dans leurs attaques.

Source : *https://bit.ly/3Zl5ckb*

Cisco

Cisco corrige des vulnérabilités de haute gravité dans les composants ACI

23 Février 2023

Cisco a informé ses clients de la disponibilité de correctifs pour deux vulnérabilités de haute gravité affectant des composants de sa solution de réseau défini par logiciel Application Centric Infrastructure (ACI).

L'une de ces failles, CVE-2023-20011, a un impact sur l'interface de gestion de l'Application Policy Infrastructure Controller (APIC) et du Cloud Network Controller de Cisco.

APIC est le point unifié d'automatisation et de gestion pour ACI.

Le deuxième problème de haute gravité, CVE-2023-20089, affecte les commutateurs Fabric de la série Cisco Nexus 9000 en mode ACI, et il peut être exploité pour des attaques par déni de service (DoS) par un attaquant adjacent non authentifié. Le fournisseur a noté que certaines conditions doivent être remplies pour l'exploitation.

En outre, Cisco a corrigé des failles de gravité moyenne dans plusieurs produits, notamment un problème logiciel UCS Manager et FXOS qui expose les fichiers de sauvegarde, un bogue d'injection de commande dans NX-OS, une injection de commande dans les Firepower Appliances et une vulnérabilité de contournement d'authentification dans les extensions Nexus (nécessite un accès physique).

Le géant des réseaux a également publié un avis d'information concernant un problème d'escalade des privilèges lié aux produits exécutant le logiciel NX-OS et configurés pour l'authentification SSH avec un certificat X.509v3.

Cisco a également mis à jour son avis pour CVE-2023-20032, une vulnérabilité critique récemment corrigée affectant la bibliothèque ClamAV.

La société a informé ses clients de la disponibilité d'informations techniques décrivant CVE-2023-20032 et de l'existence d'un exploit de type "proof-of-concept" (PoC). Il n'y a actuellement aucune preuve d'exploitation malveillante.

Source : *https://bit.ly/3Iw8nyv*

Microsoft

Microsoft corrige trois failles de type "zero-days" exploitées

14 Février 2023

Microsoft a publié des correctifs pour 75 vulnérabilités numérotées CVE, dont trois failles de type "zero-day" activement exploitées.

La première vulnérabilité de type "zero-day" est sous le nom CVE-2023-21715, elle permet aux attaquants de contourner une fonction de sécurité de Microsoft Publisher : Les politiques de macro d'Office utilisées pour bloquer les fichiers non fiables ou malveillants.

La deuxième vulnérabilité est répertoriée sous le nom CVE-2023-23376, elle est repérée dans le système de fichiers journaux communs de Windows qui pourrait permettre aux attaquants d'obtenir les privilèges SYSTEM sur un hôte cible.

La dernière vulnérabilité de type "zero-day" est CVE-2023-21823, une faille dans le composant graphique de Windows et pourrait conduire à l'exécution de code à distance et à une prise de contrôle totale d'un système vulnérable.

Microsoft n'a partagé aucun détail sur les attaques dans lesquelles ces vulnérabilités sont exploitées.

Microsoft Store mettra automatiquement à jour les clients concernés. Ceux qui ont désactivé les mises à jour automatiques doivent les obtenir via le Microsoft Store (allez dans : Library > Get updates > Update all).

Il est conseillé aux administrateurs de corriger rapidement une autre vulnérabilité critique dans Microsoft Word répertoriée sous le nom CVE-2023-21716 qui peut être exploité par le système en ouvrant simplement le volet de visualisation.

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

Chrome

Chrome 110 corrige 15 vulnérabilités

17 Février 2023

Google a annoncé que la première version stable de Chrome 110 apporte 15 correctifs de sécurité, dont 10 pour des vulnérabilités signalées par des chercheurs externes.

Parmi les bogues signalés en externe, trois sont classés comme étant de "haute gravité". Il s'agit d'un défaut de confusion de type dans le moteur V8, d'un problème d'implémentation inapproprié en mode plein écran et d'une vulnérabilité de lecture hors limites dans WebRTC.

Répertorié sous le nom de CVE-2023-0696, le premier de ces défauts de sécurité est décrit comme une corruption de tas qui peut être exploitée à distance via une page HTML élaborée. Google a versé une prime de 7 000 $ au chercheur qui a signalé le problème.

La deuxième faille de haute gravité, CVE-2023-0697, a un impact sur Chrome pour Android et pourrait permettre à un attaquant distant d'utiliser une page HTML élaborée pour usurper le contenu de l'interface utilisateur de sécurité. Google a récompensé le chercheur qui a signalé ce bogue à hauteur de 4 000 $.

CVE-2023-0698, le troisième problème, pourrait être exploité à distance via une page HTML pour effectuer une lecture de mémoire hors limites. Le chercheur qui a signalé le problème a reçu une prime de 2 000 $ pour cette découverte, indique Google dans son avis.

Chrome 110 résout également cinq vulnérabilités de gravité moyenne signalées par des chercheurs externes, notamment une faille de type use-after-free dans GPU, un bogue d'implémentation inapproprié dans Download, un défaut de débordement de tampon de tas dans WebUI et deux problèmes de confusion de type dans Data Transfer et DevTools.

Google affirme avoir distribué plus de 26 000 dollars de primes aux chercheurs qui ont signalé ces problèmes.

Le géant de l'Internet ne mentionne pas que l'une de ces vulnérabilités ait été exploitée dans des attaques.

La dernière version de Chrome est distribuée aux utilisateurs sous la forme des versions 110.0.5481.77/.78 pour Windows et 110.0.5481.77 pour Mac et Linux.

Les versions iOS et Android du navigateur ont été mises à jour respectivement en 110.0.5481.83 et 110.0.5481.63/.64.

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

Actualité

11 000 sites piratés dans une attaque par porte dérobée

Les chercheurs de Sucuri (une entreprise de cybersécurité) ont signalé une porte dérobée qui a réussi à infecter environ 11 000 sites Web au cours des derniers mois.

Selon les recherches de Sucuri, la porte dérobée redirige les utilisateurs vers des sites qui affichent des vues frauduleuses des annonces Google AdSense. Le scanner à distance SiteCheck de la société a détecté plus de 10 890 sites infectés. L'activité s'est encore intensifiée récemment, avec 70 nouveaux domaines malveillants déguisés en légitimes en 2023 et 2 600 sites infectés découverts sur le web.

Tous les sites infectés détectés par Sucuri utilisaient le CMS WordPress. Un script PHP obscurci a été injecté dans les fichiers légitimes des sites Web, tels que index.php, wp-activate.php, wp-signup.php et wp-cron.php, etc.

Environ 75 domaines à URL pseudo-courtes associés à du trafic détourné ont été découverts au cours des deux derniers mois par les chercheurs de Sucuri. Il convient de noter que presque toutes les URL malveillantes semblent faire partie du même service de raccourcissement d'URL. Certaines utilisent même des noms de services de raccourcissement populaires comme Bitly.

Les sites Web basés sur le CMS Question2Answer sont utilisés pour créer une variété de sites Web de mauvaise qualité, et les sujets de discussion y sont généralement la blockchain ou les crypto-monnaies.

Selon les chercheurs, une fraude ICO de type "pump-and-dump" peut être utilisée pour faire de la publicité frauduleuse pour de nouvelles pièces. Mais les analystes sont clairs sur le fait que l'objectif principal de cette fraude publicitaire est d'augmenter artificiellement le trafic vers les sites web qui ont l'identifiant AdSense, permettant l'affichage de la publicité Google pour la monétisation.

Un code obscurci est parfois ajouté par certains de ces sites Web malveillants à "wp-blog-header.php". Pour que le malware échappe aux efforts de nettoyage, ce code fonctionne comme une porte dérobée. Pour ce faire, il s'insère dans des fichiers qui se lancent dès que le serveur ciblé est redémarré.

L'injection supplémentaire du malware, qui se trouve dans le fichier wp-blog-header.php, s'exécutera à chaque chargement du site Web et le réinfectera. Cela permet de s'assurer que l'environnement est infecté jusqu'à ce que l'infection soit complètement supprimée.

Le malware cache sa présence en suspendant les redirections lorsqu'un visiteur se connecte en tant qu'administrateur ou visite un site infecté dans les 2 à 6 heures. Le code malveillant est masqué à l'aide du codage Base64.

Lorsque l'utilisateur entre des noms de domaine dans son navigateur, il est redirigé vers un véritable service de raccourcissement d'URL, par exemple, Cuttly ou Bitly, mais ce ne sont pas de véritables raccourcisseurs d'URL publics. Chaque domaine possède quelques URL fonctionnelles qui redirigent les visiteurs vers des sites de questions-réponses spammés avec monétisation AdSense.

Source : *http://bit.ly/41p2D2e*

Des pirates volent des jeux et des données d'employés d'Activision

Le groupe de cybersécurité et de recherche sur les logiciels malveillants vx-underground a publié des captures d'écran de données prétendument volées à Activision, notamment le calendrier des contenus prévus pour le célèbre jeu de tir à la première personne Call of Duty.

Le blogue de jeux Insider Gaming a déclaré qu'il confirmait une violation de données après avoir obtenu "l'intégralité" des données volées, qui n'ont pas été publiées par vx-underground.

Le site web affirme que les pirates ont pris des informations sur les employés, notamment "les noms complets, les emails, les numéros de téléphone, les salaires, les lieux d'emploi, les adresses, et plus encore."

TechCrunch n'a pas été en mesure de vérifier la véracité des informations divulguées ou les spécificités du piratage.

"La sécurité de nos données est essentielle, et nous avons mis en place des processus de sécurité de l'information complets pour maintenir leur confidentialité", a déclaré Joseph Christinat, porte-parole d'Activision. "notre équipe de sécurité de l'information s'est rapidement penchée sur une tentative d'hameçonnage par SMS et l'a rapidement résolue. Après une enquête approfondie, nous avons déterminé qu'aucune donnée sensible des employés, aucun code de jeu ou aucune donnée de joueur n'a été consulté."

Dans un tweet, vx-underground a écrit qu'Activision a été violé le 4 décembre, après que les pirates ont "réussi à hameçonner un utilisateur privilégié sur le réseau."

Riot Games a révélé une brèche dans laquelle des pirates ont accédé à l'"environnement de développement" de la société, ce qui leur a permis de voler le code source des jeux populaires League of Legends et Teamfight Tactics, ainsi que le code source de l'ancien système anti-triche de la société.

En 2022, selon la société de cybersécurité Group-IB, au moins 130 entreprises ont été attaquées par le collectif de pirates 0ktapus (également connu sous le nom de Scattered Spider). Le groupe s'est fait connaître en s'introduisant dans Twilio, une startup spécialisée dans les communications en nuage qui offre à d'autres entreprises des services tels que l'envoi de SMS automatisés à leurs clients. De nombreux développeurs de jeux, dont Riot Games et Epic Games, figurent parmi les 130 entreprises visées.

Source : *http://bit.ly/3IzYTY0*

LastPass : Un ingénieur DevOps s'est fait pirater pour voler des données de coffre-fort de mots de passe

LastPass a rendu publiques de nouvelles informations sur une "deuxième attaque organisée" par un acteur de la menace qui a accédé aux serveurs de stockage en cloud d'Amazon AWS et y a volé des données pendant plus de deux mois.

Selon une attaque annoncée par LastPass, les acteurs de la menace ont obtenu des données partiellement cryptées de coffre-fort des mots de passe et des informations sur les clients.

L'organisation a maintenant révélé comment les acteurs de la menace ont mené cette attaque, affirmant qu'ils l'ont fait en utilisant l'ordinateur d'un ingénieur DevOps senior pour installer un keylogger en utilisant les informations volées dans une violation de données en août, des informations provenant d'une autre violation de données et une vulnérabilité d'exécution de code à distance.

Selon LastPass, les informations volées lors de la première violation ont été utilisées lors de cette deuxième tentative coordonnée d'accès aux fichiers cryptés Amazon S3 de l'entreprise.

L'acteur de la menace a choisi l'un des quatre ingénieurs DevOps de LastPass car ils étaient les seuls à avoir accès aux clés de décryptage. Au final, les pirates ont réussi à installer un keylogger sur l'appareil de l'employé en profitant d'une faille d'exécution de code à distance dans un logiciel multimédia d'un tiers.

Selon une toute nouvelle alerte de sécurité publiée aujourd'hui, "l'acteur de la menace a pu capturer le mot de passe principal de l'employé au moment de sa saisie, après que l'employé se soit authentifié avec MFA, et obtenir l'accès au coffre-fort d'entreprise LastPass de l'ingénieur DevOps."

Après cela, l'acteur de la menace a exporté les entrées du coffre-fort d'entreprise natif et le contenu du dossier partagé, qui contenait des notes sécurisées chiffrées avec les clés d'accès et de déchiffrement nécessaires pour accéder aux sauvegardes de production AWS S3 LastPass, à d'autres ressources de stockage dans le cloud et à certaines sauvegardes de base de données critiques connexes.

L'utilisation d'informations d'identification valides a rendu difficile la détection de l'activité de l'acteur de la menace par les enquêteurs de l'entreprise, ce qui a permis au pirate d'accéder aux serveurs de stockage dans le cloud de LastPass et d'y voler des données pendant plus de deux mois, entre le 12 août 2022 et le 26 octobre 2022.

LastPass a finalement détecté le comportement anormal par le biais des alertes AWS GuardDuty lorsque l'acteur de la menace a tenté d'utiliser les rôles de gestion des identités et des accès (IAM) du cloud pour effectuer une activité non autorisée.

L'entreprise dit avoir depuis mis à jour sa posture de sécurité, notamment en faisant tourner les informations d'identification sensibles et les clés/tokens d'authentification, en révoquant les certificats, en ajoutant une journalisation et des alertes supplémentaires, et en appliquant des politiques de sécurité plus strictes.

LastPass a publié des informations plus détaillées sur les données des clients qui ont été volées lors de l'attaque.

Selon un client particulier, ces données sont très variées, comprenant des données d'authentification multifactorielle (MFA), des secrets d'intégration d'API MFA et des clés de composants de connaissances ("K2") pour les clients de Federated Business.

Source : *http://bit.ly/3SCIr97*

Bon à savoir

Les employés contournent les consignes de cybersécurité pour atteindre les objectifs de l'entreprise

L'entreprise américaine de conseil et de recherche dans le domaine des techniques avancées Gartner prévoit que d'ici 2025, le manque de talent ou l'échec humain seront responsables de plus de la moitié des cyberincidents importants. Le nombre de cyberattaques et d'attaques d'ingénierie sociale contre les personnes explose, les acteurs de la menace considérant de plus en plus les humains comme le point d'exploitation le plus vulnérable.

Une enquête de Gartner en Mai et Juin 2022 auprès de 1 310 employés a révélé que :

- 69 % des employés ont contourné les consignes de cybersécurité de leur organisation au cours des 12 derniers mois.
- Les programmes de cybersécurité axés sur la conformité, le faible soutien de la direction et une maturité inférieure à celle du secteur sont autant d'indicateurs d'une organisation qui ne considère pas la gestion des risques de sécurité comme essentielle au succès de l'entreprise.
- Les frictions qui ralentissent les employés et conduisent à des comportements non sécurisés sont un facteur important de risque interne.
- Les professionnels de la cybersécurité sont confrontés à des niveaux de stress insoutenable.
- Les professionnels de la cybersécurité sont sur la défensive, avec pour seules issues possibles qu'ils ne soient pas piratés ou qu'ils le soient. L'impact psychologique de cette situation affecte directement la qualité des décisions et les performances des responsables de la cybersécurité et de leurs équipes.

Pour faire face à cette menace croissante, Gartner prévoit que :

- La moitié des moyennes et grandes entreprises adopteront des programmes formels de gestion du risque d'initié d'ici 2025, contre 10 % actuellement.

- Un programme ciblé de gestion du risque d'initié doit identifier de manière proactive et prédictive les comportements susceptibles d'entraîner l'exfiltration potentielle d'actifs de l'entreprise ou d'autres actions dommageables et fournir des conseils correctifs, et non des sanctions.
- Les RSSI doivent de plus en plus prendre en compte le risque d'initié lors de l'élaboration d'un programme de cybersécurité.
- Les outils de cybersécurité traditionnels n'ont qu'une visibilité limitée des menaces qui viennent de l'intérieur

Source : *https://bit.ly/3kzjY8cu*

Evènements

Evènement du mois

Webinaire -Attaque et Défense- Protection du cloud

27 Février 2023

Online

https://bit.ly/3IXjS3z

Les cybercriminels ciblent les environnement cloud car c'est là ou les données les plus précieuses sont stockées. Dans cet épisode d'attaque et de défense, ils vont plonger dans plusieurs événements réels de violation d'infrastructure en nuage.

L'objectif de ce webinaire est de déconstruire les outils, tactiques et procédures des attaquants qui ont permis une compromission réussie du cloud, et d'identifier les stratégies de défense qui peuvent être adoptées pour réduire le risque pour les opérations en nuage.

Evènement à venir

Événement de partage des connaissances CSA HKM - Mars 2023

02 Mars 2023

Online

https://bit.ly/3ZjSMc4

La cybersécurité dans le Cloud Computing est en constante évolution.

L'objectif de cet événement est d'aborder le sujet brûlant dans le monde informatique ChatGPT, expliquer les fonctions de ce dernier avec une démonstration et sa relation avec le Cloud Computing et le domaine de la cybersécurité, et explorer comment ChatGPT peut aider notre industrie de la cybersécurité.

Cet événement se déroulera en ligne avec un accès gratuit le 02 Mars 2023.

Référence	ANPT-2023-BV-02
Titre	Bulletin de veille N°02
Date de version	28 Février 2023
Contact	ssi@anpt.dz