BULLETIN DE VEILLE N°08

ANPT-2023-BV-08

"One single vulnerability is all an attacker needs"
-- Window Snyder --

Août 2023

Alertes de sécurité

Cisco

Cisco corrige des vulnérabilités de haute gravité dans les applications d'entreprise

21 Août 2023

Cisco a récemment annoncé des mises à jour de sécurité pour diverses applications d'entreprise, visant à corriger des vulnérabilités critiques qui pourraient entraîner des problèmes graves tels que l'escalade des privilèges, l'injection SQL, la traversée de répertoire et les attaques par déni de service (DoS).

Parmi ces vulnérabilités, la plus grave affecte l'interface de gestion web de deux applications Cisco : Cisco Unified Communications Manager (Unified CM) et Unified Communications Manager Session Management Edition (Unified CM SME).

Cette vulnérabilité, répertoriée sous le nom de CVE-2023-20211 avec un score CVSS de 8.1, provient d'une mauvaise validation des données fournies par l'utilisateur. Cette faille pourrait potentiellement permettre à un attaquant distant et authentifié d'exécuter une attaque par injection SQL.

Cisco a corrigé la faille en publiant les versions 12.5(1)SU8 de Unified CM et Unified CM SME et a également publié un fichier correctif pour la version 14 des applications.

Le géant de la technologie prévient que le code d'exploitation de la preuve de concept (PoC) ciblant la vulnérabilité a été publié.

En outre, Cisco a également publié des correctifs pour CVE-2023-20224, une vulnérabilité qui permet l'élévation des privilèges dans le type d'installation de l'appliance virtuelle de ThousandEyes Enterprise Agent. Cette vulnérabilité provient également d'une validation inadéquate des données d'entrée fournies par l'utilisateur. Si elle était exploitée, elle permettrait à un attaquant de s'authentifier sur un appareil affecté par le biais de commandes soigneusement élaborées, ce qui lui permettrait d'exécuter des commandes avec les privilèges de l'administrateur. Cisco souligne que pour cette vulnérabilité, l'attaquant a besoin d'informations d'identification valides. Ce bogue a été résolu dans la version 0.230 de ThousandEyes Enterprise Agent.

Un autre problème lié à une validation insuffisante des entrées a été découvert dans l'application Duo Device Health, permettant potentiellement aux attaquants de mener des attaques par traversée de répertoire et d'écraser des fichiers arbitraires. Cette vulnérabilité, identifiée comme CVE-2023-20229, a été corrigée dans la version 5.2.0 de l'application.

En outre, Cisco a introduit des correctifs pour deux vulnérabilités DoS dans ClamAV, une boîte à outils antimalware gratuite intégrée dans divers produits Cisco. La première vulnérabilité, CVE-2023-20197, a été identifiée dans l'analyseur d'images du système de fichiers de ClamAV pour Hierarchical File System Plus (HFS+). Cisco a observé la publication d'un code de preuve de concept accessible au public et ciblant cette vulnérabilité.

Bien qu'aucune attaque malveillante exploitant ces vulnérabilités n'ait été signalée, Cisco recommande vivement aux utilisateurs de mettre rapidement à jour leurs installations.

Source : *https://bit.ly/44yhMi5*

NVIDIA

Trois failles dans NVIDIA peuvent entraîner une corruption de la mémoire

23 Août 2023

Google Cisco Talos a récemment révélé trois vulnérabilités dans la fonctionnalité shader du pilote NVIDIA D3D10 qui fonctionne avec les cartes graphiques de NVIDIA.

Le pilote est vulnérable à la corruption de la mémoire si un adversaire envoie un packer de shaders spécialement conçu, ce qui peut entraîner un problème de corruption de la mémoire dans le pilote.

Les trois problèmes, identifiés comme CVE-2022-34671, CVE-2022-34671 et CVE-2022-34671, ont une note de gravité CVSS de 8,5 sur 10.

Un attaquant pourrait exploiter ces vulnérabilités à partir de machines invitées utilisant des environnements de

virtualisation (tels que VMware, QEMU et VirtualBox) pour effectuer une évasion de l'invité vers l'hôte.

Les recherches de Talos indiquent également que ces vulnérabilités pourraient être déclenchées à partir d'un navigateur web utilisant WebGL et WebAssembly. Les chercheurs de l'entreprise ont déclenché ces problèmes à partir d'un invité HYPER-V utilisant la fonction RemoteFX, ce qui a conduit à l'exécution d'un code vulnérable sur l'hôte HYPER-V (à l'intérieur du processus rdvgm.exe). Microsoft a récemment supprimé RemoteFX, mais des machines plus anciennes peuvent encore utiliser ce logiciel.

Talos a travaillé avec NVIDIA pour s'assurer que ces vulnérabilités sont résolues et qu'une mise à jour est disponible pour les clients concernés.

Source : *https://bit.ly/45AzvXA*

Google

Chrome : Mise à jour de sécurité pour corriger des failles de haute gravité

23 Août 2023

Google a introduit une mise à jour de sécurité pour Chrome 116, qui corrige cinq vulnérabilités en matière de sécurité de la mémoire signalées par des chercheurs externes. Parmi ces problèmes, quatre ont été classés comme ayant un niveau de gravité élevé.

La plus importante de ces vulnérabilités est identifiée sous le nom de CVE-2023-4430, qui concerne un bogue "use-after-free" trouvé dans Vulkan. Vulkan est une norme ouverte multiplateforme pour les graphiques 3D. Cette vulnérabilité a été révélée par Cassidy Kim, qui a ensuite reçu une prime de 10 000 dollars de la part de Google.

Un autre problème notable lié à l'utilisation après la mort est enregistré sous le nom de CVE-2023-4429. Ce problème spécifique se situe dans le composant Loader. Un chercheur anonyme a découvert et signalé cette faille, et Google l'a récompensé par une prime de 3 000 dollars pour ses découvertes.

En outre, une vulnérabilité d'accès à la mémoire hors limites de haute sévérité dans CSS a donné lieu à une prime de 2 000 dollars de la part de Google.

Toutefois, il est important de noter que la politique de Google stipule qu'aucune prime ne sera accordée pour un problème similaire découvert dans le moteur JavaScript V8, qui a été signalé par un chercheur du Google Project Zero. De même, une faille d'accès à la mémoire hors limites de gravité moyenne dans Fonts, signalée par un chercheur en sécurité de Microsoft, ne pourra pas non plus faire l'objet d'un bug bounty.

Cette dernière version de Chrome est déployée sous la forme de la version 116.0.5845.110 pour les plateformes Mac et Linux, tandis que les utilisateurs de Windows recevront les versions 116.0.5845.110/.111.

Il convient de préciser que Google n'a détecté aucun cas d'exploitation de ces vulnérabilités dans le cadre d'attaques.

Source : *https://bit.ly/47WtPZw*

WinRAR

WinRAR : Une faille de type zero-Day activement exploité pour diffuser des logiciels malveillants

25 Août 2023

Une vulnérabilité d'exécution de code à distance zero-day récemment découverte dans WinRAR a été activement exploitée dans la nature pour diffuser diverses familles de logiciels malveillants, dont DarkMe, GuLoader et RemcosRAT. Selon les chercheurs du Group-IB, ces attaques utilisant la vulnérabilité se poursuivent depuis le mois d'avril.

La détection de cette attaque a eu lieu lors de la surveillance par Group-IB des activités des logiciels malveillants DarkMe. Bien que DarkMe ait été lié au groupe financier Evilnum, l'identité de la partie qui exploite la vulnérabilité WinRAR pour déployer le logiciel malveillant reste incertaine.

Les auteurs de la menace ont distribué des archives zip malveillantes par l'intermédiaire d'au moins huit forums publics couramment fréquentés par les commerçants en ligne. En outre, on a découvert des cas où les attaquants ont utilisé un service de stockage de fichiers gratuit appelé catbox.moe pour distribuer ces archives zip. Une fois le logiciel malveillant implanté sur un système, il obtient un accès non autorisé aux comptes de trading des victimes et initie des transactions non autorisées, facilitant ainsi le retrait des fonds. Malgré les efforts des administrateurs du forum pour détecter et bloquer les fichiers et les comptes malveillants, les attaquants ont réussi à contourner ces mesures, perpétuant la distribution de fichiers nuisibles par le biais de messages privés aux utilisateurs. Les administrateurs du forum avaient également alerté les utilisateurs sur les tentatives d'attaque en cours. Jusqu'à présent, cette campagne a touché les appareils de 130 commerçants.

La vulnérabilité zero-day, désignée sous le nom de CVE-2023-3881, permet aux attaquants de manipuler les extensions de fichiers. Cette manipulation leur permet de camoufler du code malveillant dans des archives zip en les présentant comme des fichiers jpg, txt ou d'autres formats bénins. L'exploit est déclenché lorsque les victimes ouvrent le fichier leurre contenu dans ces archives. Cette action fait que la fonction ShellExecute de WinRAR reçoit un paramètre incorrect.

Il est fortement conseillé aux utilisateurs de mettre à jour rapidement leur système avec la dernière version (6.23) de WinRAR.

Source : *https://bit.ly/47Wu3Qm*

Actualité

Publication de 2,6 millions de données d'utilisateurs de Duolingo sur un forum de piratage

Les données personnelles de 2,6 millions d'utilisateurs de Duolingo, une importante plateforme d'apprentissage des langues, ont été exposées sur un forum de piratage. Cette fuite de données a permis à des acteurs malveillants de lancer des attaques de phishing ciblées en utilisant les informations compromises.

Duolingo dispose d'une vaste base d'utilisateurs de plus de 74 millions de personnes dans le monde qui s'adonnent à l'apprentissage des langues. En janvier 2023, un individu a tenté de vendre les données volées de 2,6 millions d'utilisateurs de Duolingo sur le forum de piratage Breached, qui a depuis été fermé. Cet ensemble de données, que l'on peut obtenir pour 1 500 dollars, comprend une combinaison de noms de connexion publics et de noms réels, ainsi que des données non publiques, notamment des adresses électroniques et des détails internes concernant les services de Duolingo.

Bien que les noms réels et les identifiants de connexion soient généralement accessibles via le profil Duolingo d'un utilisateur, l'inclusion d'adresses électroniques dans les informations divulguées soulève de plus grandes inquiétudes en raison du potentiel d'exploitation dans le cadre de cyberattaques. Interrogé sur l'incident, Duolingo a confirmé que les données provenaient de profils accessibles au public et a indiqué qu'il examinait si des mesures de sécurité supplémentaires étaient nécessaires. Toutefois, la question des adresses électroniques faisant partie des données exposées n'a pas été explicitement abordée.

Les données divulguées ont été obtenues à l'aide d'une interface de programmation d'applications (API) accessible au public et partagée ouvertement depuis mars 2023. Les chercheurs avaient démontré publiquement l'utilisation de cette API. Elle permet aux individus de saisir un nom d'utilisateur et d'obtenir un résultat JSON contenant les détails du profil public de l'utilisateur correspondant. L'API peut également être utilisée avec des adresses électroniques pour confirmer leur association avec un compte Duolingo valide.

Bien que l'abus de cette API ait été signalé à Duolingo en janvier, elle reste accessible à tout le monde sur l'internet. L'API a permis au pirate de données de saisir des millions d'adresses électroniques, provenant probablement de violations de données antérieures, et de vérifier si elles correspondaient à des comptes Duolingo. Ce processus a abouti à la création d'un ensemble de données comprenant à la fois des informations publiques et non publiques.

En outre, un autre acteur de la menace a partagé ses propres résultats de grattage de l'API, mettant en évidence certains champs qui indiquent des utilisateurs ayant des privilèges élevés dans le système de Duolingo. Ces utilisateurs sont particulièrement intéressants pour les acteurs de la menace qui mènent des attaques par hameçonnage.

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

Encore une fois, Burger King oublie de mettre un mot de passe sur ses systèmes !

Burger King, géant international de la restauration rapide dont le siège est aux États-Unis, exploite un vaste réseau de plus de 19 000 restaurants dans le monde entier, générant un chiffre d'affaires substantiel de 1,8 milliard de dollars.

Récemment, les chercheurs de Cybernews sont tombés sur une faille de sécurité importante sur le site web français de Burger King. Cette faille a été attribuée à une mauvaise configuration, ce qui a conduit à l'exposition d'informations d'identification sensibles au public. Si ces informations d'identification divulguées étaient tombées entre les mains d'individus malveillants, elles auraient pu devenir un outil puissant pour mener des cyber-attaques contre les systèmes de Burger King.

Malheureusement, ce n'est pas la première fois que Burger King est impliqué dans un incident d'exposition de données. En 2019, à la suite d'une erreur de configuration similaire, la filiale française de la chaîne a divulgué par inadvertance des informations personnelles identifiables (PII) appartenant à des enfants qui avaient acheté des repas chez Burger King.

Alerté par l'équipe de Cybernews, Burger King s'est rapidement penché sur le problème et a rectifié la mauvaise configuration.

Le 1er juin 2023, l'équipe de recherche de Cybernews a dévoilé un fichier d'environnement (.env) accessible au public et associé au site web français de Burger King.

Ce fichier se trouvait dans un sous-domaine dédié à la publication d'offres d'emploi. Bien que les données exposées n'aient pas suffi à elles seules à prendre le contrôle du site web, elles auraient pu simplifier considérablement le processus pour les attaquants potentiels, en particulier s'ils parvenaient à repérer d'autres points vulnérables.

Parmi les informations sensibles contenues dans le fichier figuraient les identifiants d'une base de données. Bien que des contraintes juridiques aient empêché les chercheurs d'examiner le contenu exact de la base de données, celle-ci contenait probablement des offres d'emploi et potentiellement d'autres informations soumises par les candidats. L'exposition des informations d'identification d'une base de données était particulièrement précaire, car des acteurs malveillants pouvaient les utiliser pour établir une connexion avec la base de données et manipuler ou extraire les données stockées. Si ces acteurs identifiaient et exploitaient une vulnérabilité d'exécution de code PHP sur le site, les informations d'identification du fichier .env pourraient faciliter une extraction plus subreptice de la base de données MySQL.

Source : *https://bit.ly/3EHA8D3*

Discord informe les utilisateurs d'une violation de données affectant 180 comptes

Les Le populaire serveur de communication Discord, qui regroupe environ 150 millions d'utilisateurs mensuels, a récemment commencé à informer un sous-ensemble de sa base d'utilisateurs d'une violation de données commise au mois de mars.

La violation, qui a été publiquement reconnue par Discord en mai 2023, a touché un total de 180 comptes, selon une notification de violation de données déposée auprès du bureau du procureur général du Maine.

Cet incident contraste avec la récente violation du service tiers Discord.io, qui a touché 760 000 utilisateurs et entraîné la fermeture temporaire du site web.

Discord.io, une plateforme permettant aux utilisateurs de Discord de générer des liens personnalisés pour leurs canaux, a subi une violation majeure le 14 août. L'attaquant a exploité une vulnérabilité dans le code du site web et a ensuite vendu aux enchères les données volées, y compris les mots de passe hachés, les informations de facturation et les identifiants Discord.

Suite à cette violation, Discord.io a suspendu ses services. L'entreprise s'est engagée à procéder à une révision complète du code et des pratiques de sécurité de son site web afin de renforcer ses mécanismes de défense contre de futures violations.

Alors que l'incident de Discord.io touche principalement les informations personnelles des utilisateurs, la fuite du mois de mars concernait la compromission du compte d'un agent du service d'assistance à la clientèle. Cette fuite a permis à des acteurs malveillants d'accéder aux adresses électroniques des utilisateurs, aux tickets d'assistance et aux communications échangées avec l'équipe d'assistance de Discord.

Les informations communiquées par Discord au bureau du procureur général de l'État du Maine comprenaient une enquête approfondie sur les tickets d'assistance compromis. Les résultats ont révélé que les informations personnelles d'au moins un résident du Maine, comprenant son nom et son numéro de permis de conduire ou de carte d'identité de l'État, avaient été exposées. Ces informations ont ensuite été utilisées pour informer les personnes concernées.

Discord prend des mesures proactives pour renforcer son infrastructure de sécurité. En plus d'améliorer la sécurité de sa plateforme pour protéger sa base d'utilisateurs, Discord fournit également des services de surveillance du crédit et de protection contre le vol d'identité aux utilisateurs concernés afin d'atténuer d'éventuels dommages supplémentaires.

Source : *https://bit.ly/3PoD6T1*

Bon à savoir

Ransomware : Payer ou ne pas payer

La création de stratégies et d'initiatives de sécurité globales ne doit pas seulement mettre l'accent sur la défense, mais aussi répondre à des questions cruciales telles que "Comment l'organisation va-t-elle réagir à une attaque de ransomware ?" et "Quand le paiement d'une rançon peut-il être envisagé ?"

Il faut savoir que :

- Le paiement d'une rançon peut accroître la rentabilité des attaques par ransomware, ce qui incite les cybercriminels à poursuivre leurs activités. En outre, le fait que le public ait connaissance du paiement d'une rançon peut nuire à la réputation d'une organisation et à la confiance de ses clients, car il semble soutenir les activités criminelles. Bien qu'il soit parfois inévitable, le paiement doit être envisagé avec prudence.
- Le fait de céder à une demande de rançon peut entraîner d'autres attaques, car la nouvelle du paiement circule parmi les groupes de cybercriminels. Les organisations qui choisissent de payer doivent anticiper la possibilité d'attaques futures.
- Pour certaines entreprises incapables de récupérer leurs données de manière autonome ou de reprendre leurs activités rapidement, il est essentiel d'évaluer le coût du temps d'arrêt. La compréhension de l'impact financier par heure d'indisponibilité et des pertes potentielles (atteinte à la réputation, rupture de contrat, fluctuation du cours de l'action et baisse de la productivité des employés) peut guider les décisions. Si la rançon est nettement inférieure à ces pertes potentielles, il peut sembler économiquement prudent de payer à court terme.
- Les gangs de ransomware se livrent souvent à des extorsions multiformes, volant des données pour obtenir un effet de levier supplémentaire. Malgré le paiement, la récupération des données peut être incomplète et le processus de récupération peut être long. Il est risqué de se fier aux promesses des attaquants de restituer les données.
- S'il n'est pas idéal de payer la rançon, la perte de données résultant d'une attaque peut être grave. La restauration complète des données peut prendre des mois, ce qui implique des efforts de récupération de données à forte intensité de main-d'œuvre.

Face aux menaces des ransomwares, les organisations se retrouvent souvent dans une position vulnérable. La stratégie la plus efficace comporte deux volets : la protection et la résilience.

1. Mesures de protection :

- Sensibilisation des employés aux risques et à la prévention des ransomwares.
- Gestion régulière des correctifs et tests de sécurité proactifs.
- Sauvegardes programmées et tests rigoureux des processus de récupération.
- Segmentation du réseau pour stopper la propagation latérale des attaques.

2. Résilience et réaction :

Dans le cadre d'un programme de sécurité solide, il est essentiel de mettre l'accent sur la préparation à la réponse. Les organisations devraient s'efforcer de

- Comprendre rapidement l'étendue d'un incident grâce à des analyses rapides.
- Mesurer la gravité de l'attaque pour décider s'il est préférable de payer plutôt que d'endurer les conséquences.
- Cultiver la résilience et l'adaptabilité pour contrecarrer les efforts des attaquants et réagir rapidement, en évitant de réfléchir longuement à la question de savoir s'il faut payer ou non.

En conclusion, les programmes de sécurité doivent donner la priorité à l'amélioration de la résilience et de l'agilité. En renforçant les défenses, en mettant en œuvre des réponses efficaces et en minimisant les temps d'arrêt, les organisations peuvent réduire l'incertitude entourant les attaques de ransomware, ce qui leur permet de répondre de manière décisive à la question de savoir s'il faut ou non payer la rançon.

Source : *https://bit.ly/4803ERz*

Evènements

Evènement à venir

Cybersecurity- Learning to protect your business

07 Septembre 2023

Online

https://bit.ly/481BrtC

Chaque année, un nombre croissant d'entreprises subissent les effets néfastes des cyberattaques, qui se traduisent par des pertes financières considérables dues au paiement de rançons et à des préoccupations généralisées en matière de protection de la vie privée dans le monde entier. Découvrez des stratégies efficaces pour protéger votre entreprise contre la majorité de ces attaques en mettant en œuvre des politiques simples et en utilisant des outils rentables et intelligents. Vous pourrez ainsi garantir la sécurité de vos clients et de votre propre organisation.

Référence	ANPT-2023-BV-08
Titre	Bulletin de veille N°08
Date de version	31 Août 2023
Contact	ssi@anpt.dz