BULLETIN DE VEILLE N°04

ANPT-2022-BV-04

"Technology trust is a good thing, but control is a better one."
— Stephane Nappo --

Avril 2022

Alertes de sécurité

Cisco

Une vulnérabilité de vol des informations d'identification d'administration dans Cisco Umbrella

21 Avril 2022

Cisco a publié des correctifs pour une vulnérabilité de haute gravité affectant l'Appliance virtuelle Cisco Umbrella (VA), autorisant des attaquants non authentifiés de voler les informations d'identification de l'administrateur à distance.

Cisco Umbrella est un service de sécurité en cloud utilisé par plus de 24 000 organisations comme sécurité de la couche DNS contre le phishing, les logiciels malveillants et les ransomwares.

La faille, connue sous le nom de CVE-2022-20773, existe dans le mécanisme d'authentification SSH par clé de Cisco Umbrella VA. Elle permet à un attaquant de réaliser une attaque de type 'man-in-the-middle' sur une connexion SSH pour récupérer les informations d'identification de l'administrateur et ensuite modifier les configurations ou recharger le VA.

La vulnérabilité a un impact sur le Cisco Umbrella VA pour Hyper-V et VMWare ESXi exécutant des versions logicielles antérieures à 3.3.2.

Il n'y a pas de solution de contournement ou d'atténuation disponible pour cette faille de sécurité. De ce fait, Cisco conseille à ses clients d'effectuer une mise à niveau vers une version corrigée du logiciel.

Source : *https://bit.ly/3Mu8n2m*

Multiples vulnérabilités dans Cisco Data Center Network Manager

06 Avril 2022

D'autres failles affectant le produit Cisco Nexus Dashboard Fabric Controller ont été corrigées par Cisco. Ce produit est utilisé pour administrer les réseaux pour tous les déploiements compatibles NX-OS. Les bogues permettent à un attaquant d'exécuter de code arbitraire avec les privilèges root sur les systèmes vulnérables.

Ces failles (suivies sous les noms de CVE-2017-5641 et CVE-2015-3269) se trouvent dans la configuration des autorisations de l'utilisateur. Une commande 'tcpdump' modifiée peut déclencher l'exécution d'une opération privilégiée. Un attaquant peut exploiter cette faille en conjonction avec d'autres vulnérabilités pour exécuter du code arbitraire dans le contexte de root.

On recommande aux utilisateurs de mettre à jour leurs systèmes vers la version corrigée 11.5.4 du logiciel afin d'éviter toute menace possible.

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

Tenable

Vulnérabilité corrigée dans Tenable Nessus Agent

01 Avril 2022

Tenable a publié des mises à jour de sécurité pour son produit Nessus Agent afin de corriger une vulnérabilité dans le logiciel OpenSSL qui est utilisé pour assurer le bon fonctionnement de l'agent Nessus, cette faille permet à un acteur de menace de provoquer un déni de service (DoS) à distance.

Suivie sous le nom de CVE-2022-0778 avec une gravité haute de 7.5 sur l'échelle CVSS, ce bogue est dû à un problème dans la fonction 'BN_mod_sqrt()' qui calcule une racine carrée modulaire utilisée lors de l'analyse des certificats contenant des clés publiques, cela permet à un attaquant de faire tourner cette fonction en boucle infinie en introduisant un certificat erroné, ce qui déclenche une attaque DoS.

Avec la sortie de Nessus Agent 8.3.3 et 10.1.3, les utilisateurs peuvent appliquer les correctifs afin d'atténuer tout risque possible.

Source : *https://bit.ly/3krx0RD*

Drupal

Drupal corrige deux vulnérabilités de contournement d'accès et d'écrasement de données

21 Avril 2022

Drupal a annoncé la publication de correctifs de sécurité pour résoudre quelques vulnérabilités pouvant entraîner le contournement d'accès et l'écrasement de données.

Le premier bogue corrigé dans le système open source de gestion de contenu (CMS) est contournement d'accès qui existe en raison d'une API d'accès aux entités génériques mal implémentée pour les révisions d'entités. Il affecte que la version 9.3 de Drupal, et uniquement les sites utilisant le système de révision.

La deuxième faille identifiée dans l'API de formulaire de Drupal core, elle permet à un attaquant d'injecter des valeurs non autorisées ou écraser des données. Les formulaires affectés sont peu fréquents, mais Drupal note que, dans certains cas, les failles pourraient permettre à un attaquant de modifier des données critiques ou sensibles.

Il est conseillé aux utilisateurs de mettre à jour leur site vers une version corrigée (9.3.12 ou 9.2.18) dès que possible.

Source : *https://bit.ly/3ELt2wn*

Oracle

520 nouveaux correctifs de sécurité dans le Critical Patch Update d'oracle

20 Avril 2022

Oracle a publié 520 correctifs de sécurité dans le cadre de son Critical Patch Update (CPU) d'avril 2022, dont près de 300 pour des vulnérabilités pouvant être exploitées à distance sans authentification.

Plus de 75 patchs concernent des failles de sécurité critiques, dont trois ont reçoit un score de 10 sur l'échelle d'évaluation CVSS et plus de 40 des vulnérabilités restantes ont un score CVSS compris entre 8 et 9.

Parmi les correctifs inclus dans le CPU, la faille CVE-2022-22965 également connue sous le nom de Spring4Shell ou SpringShell un bogue critique d'exécution de code à distance (RCE) dans le Framework Spring. L'un de ces correctifs résout également CVE-2022-22963, une faille critique de RCE dans la fonction Spring Cloud.

Oracle Communications a reçu le plus grand nombre de correctifs dans cette CPU trimestrielle, soit 149. Parmi les bogues résolus, 98 peuvent être exploités à distance sans authentification. D'autres applications ont reçu des mises à jour tels que Fusion Middleware, MySQL, les applications de services financiers et de communication …

La société recommande les utilisateurs et les administrateurs d'examiner le CPU et appliquer les correctifs disponibles dès que possible.

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

Juniper Networks

Juniper Networks corrige 30 vulnérabilités affectant ses produits

15 Avril 2022

Juniper Networks a publié des correctifs pour plus de 30 vulnérabilités dans ses produits, y compris des failles graves dans Contrail Networking et Junos OS, elles peuvent permettre à un attaquant de prendre le contrôle d'un système affecté.

D'après l'avis publié par la société, les vulnérabilité les plus graves sont :

- Débordement de tampon dans Pillow (CVE-2021-25289 et CVE-2021-34552) et un débordement de tas dans Apache HTTP Server (CVE-2021-26691) avec un score CVSS de 9.8.
- Un écrasement de mémoire entraînant un blocage de processus de travail dans le résolveur nginx (CVE-2021-23017) et le paquet xmlhttprequest-ssl (CVE-2021-31597) avec un score de 9.4.

Juniper a également corrigée 14 vulnérabilités dans Junos OS et Junos OS Evolved, dont 10 problèmes classés " haute gravité ", qui pourraient conduire à une exécution de code ou à un déni de service, dans certaines conditions.

La société déclare qu'aucune de ces failles n'a été exploité dans le cadre d'attaques, mais elle encourage ses client d'appliquer les mises à jour dès que possible.

Source : *https://bit.ly/3xRajy3*

VMware

Des failles critiques d'exécution de code touchent les produits VMware

14 Avril 2022

VMware a déployé des correctifs pour une faille de sécurité extrêmement critique dans le produit VMWare Cloud Director, avertissant que les systèmes non corrigés sont exposés à des attaques par exécution de code à distance.

Répertoriée sous le nom de CVE-2022-22966, la vulnérabilité a reçu un score de 9.1 et peut permettre à un acteur malveillant authentifié avec un haut niveau de privilège d'exécuter de code à distance pour accéder au serveur.

Un autre bogue a été corrigé par VMware, qui est a été exploité dans des attaques réelles. Ce problème affecte le produit VMware Workspace ONE Access and Identity Manager avec un score CVSS de 9,8. Connue sous le code de CVE-2022-22954, elle peut déclencher une injection de modèle côté serveur qui peut entraîner l'exécution de code à distance.

La société avère ses clients de gravité de ses problèmes et les encourages à mettre à jour leurs systèmes afin d'éliminer les menaces potentielles.

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

Actualité

Des serveurs Microsoft Exchange piratés pour déployer un ransomware

Un ransomware affilié à Hive a ciblé les serveurs Microsoft Exchange vulnérables aux problèmes de sécurité de ProxyShell pour déployer diverses portes dérobées comme Cobalt Strike.

À partir de là, les acteurs de la menace effectuent une reconnaissance du réseau, volent les informations d'identification du compte administrateur, exfiltrent des données précieuses, pour finalement déployer la charge utile de cryptage de fichiers.

ProxyShell est un ensemble de trois vulnérabilités dans le serveur Microsoft Exchange, répertoriées sous les noms de CVE-2021-34473, CVE-2021-34523 et CVE-2021-31297, qui permettent l'exécution de code à distance sans authentification sur les déploiements vulnérables.

Après l'exploitation de ProxyShell, les pirates ont implanté quatre shells web dans un répertoire Exchange accessible et ont exécuté du code PowerShell avec des privilèges élevés pour télécharger des stagers Cobalt Strike.

À partir de là, les intrus ont utilisé Mimikatz, un voleur d'informations d'identification, pour arracher le mot de passe d'un compte administrateur de domaine et effectuer un mouvement latéral, en accédant à d'autres ressources du réseau.

Ensuite, les acteurs de la menace ont effectué des opérations de recherche de fichiers étendues pour localiser les données les plus précieuses afin de pousser la victime à payer une rançon plus importante.

Enfin, après l'exfiltration de tous les fichiers, un ransomware nommé "Windows.exe" a été déposé et exécuté sur plusieurs appareils.

Avant de crypter les fichiers de l'organisation, la charge utile Golang a supprimé les copies d'ombre, désactivé Windows Defender, effacé les journaux d'événements Windows, tué les processus de liaison de fichiers et arrêté le gestionnaire de comptes de sécurité pour neutraliser les alertes.

***Source** : https://bit.ly/3xU0Mq3*

Des chercheurs affirment que Webex surveille le microphone même lorsqu'il est coupé

Selon des chercheurs de l'Université du Wisconsin-Madison et de l'Université Loyola de Chicago, les applications de vidéoconférence (VCA) les plus répandues, y compris celles utilisées dans les environnements d'entreprise, peuvent interroger activement le microphone, même lorsque l'utilisateur est en sourdine.

Les chercheurs ont découvert non seulement que certaines applications surveillent en permanence l'entrée du microphone lorsque le participant est en sourdine, mais aussi que les données télémétriques qu'elles transmettent à leurs serveurs peuvent être utilisées pour identifier avec précision différents types d'activités de fond effectuées par les utilisateurs.

"Il est intéressant de noter que, tant sous Windows que sous macOS, nous avons constaté que Cisco Webex interroge le microphone indépendamment de l'état du bouton muet", indiquent les chercheurs. "Nous avons découvert que lorsque l'application était muette, le tampon audio de Webex contenait de l'audio brut provenant du microphone."

Les chercheurs ont également découvert que Webex - qui est le seul projet "qui échantillonne continuellement le microphone alors que l'utilisateur est en sourdine" - envoyait des données télémétriques dérivées de l'audio à ses serveurs, minute par minute. Ils ont réussi à intercepter "les [données] en clair immédiatement avant qu'elles ne soient transmises à l'API de socket réseau de Windows" et les ont utilisées pour prendre des empreintes digitales des activités de l'utilisateur en arrière-plan.

Dans un communiqué, Cisco précise que les données collectées étaient limitées aux paramètres audio.

"En janvier 2022, des chercheurs ont découvert que des données de paramètres audio telles que le volume et le gain - et non des voix ou des sons réels - étaient détectées et collectées lorsque les utilisateurs étaient muets dans les réunions Webex. Ces données étaient destinées à prendre en charge l'expérience utilisateur (par exemple les notifications de mise en sourdine, l'annulation du bruit de fond, l'optimisation du volume) et le dépannage", a déclaré la société.

"En janvier 2022, Webex a arrêté la collecte de données sur les paramètres audio relatives au dépannage lorsque les utilisateurs sont en sourdine ; les clients de Webex peuvent contacter Cisco pour désactiver la détection restante des paramètres audio, qui sont nécessaires pour les fonctionnalités que nous fournissons même lorsqu'un utilisateur est en sourdine, comme la notification de sourdine et l'annulation de l'écho. Nous apprécions les commentaires de nos clients, chercheurs et autres parties prenantes qui nous aident à améliorer nos produits", a ajouté Cisco.

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

Une campagne de cybercriminalité visant le secteur bancaire africain

Une série d'attaques a été signalée dans toute l'Afrique de l'Ouest, les attaquants se faisant passer pour des employeurs potentiels pour inciter les victimes à télécharger des fichiers malveillants.

Les chercheurs de HP Wolf Security, qui ont suivi la campagne, ont noté qu'ils ont repéré les attaques pour la première fois au "début de l'année 2022", lorsqu'un employé d'une banque ouest-africaine anonyme a reçu un courriel prétendant provenir d'un

recruteur d'une autre banque africaine et contenant des informations sur des offres d'emploi.

En enquêtant, les chercheurs ont découvert que le domaine utilisé pour envoyer l'e-mail était typosquatté et n'appartenait pas à l'organisation imitée.

Les e-mails contenaient des fichiers HTML qui, s'ils étaient ouverts, invitaient l'utilisateur à télécharger un fichier ISO, lequel contenait à son tour un script Visual Basic qui exécutait le malware.

Cette technique, appelée HTML smuggling, permet aux attaquants de faire passer des fichiers malveillants sans passer par la sécurité des passerelles de messagerie.

Patrick Schläpfer, un analyste des logiciels malveillants chez HP Wolf Security, a déclaré que, bien que l'équipe de recherche ne sache pas pourquoi l'Afrique en particulier a été ciblée, les institutions financières offrent généralement "un degré élevé d'opportunités pour les cybercriminels de monétiser l'accès et les données volées s'ils réussissent à compromettre le réseau d'une banque".

Schläpfer ajoute : "Dans cette campagne, les attaquants ont utilisé une combinaison de techniques d'attaque. Nous recommandons aux entreprises de faire attention aux abus de marque, notamment aux sites Web typosquattés qui usurpent l'identité de leur marque.

"S'ils sont découverts, ils doivent être signalés au fournisseur d'hébergement et au registraire de domaine dès que possible.

"En outre, les organisations doivent également s'assurer qu'elles ont une visibilité sur leur réseau afin d'isoler ou de bloquer les comportements de processus malveillants. Ces recommandations s'appliquent à toutes les organisations, et pas seulement au secteur bancaire en Afrique."

Source : *https://bit.ly/3Kkl26y*

Des serveurs Docker piratés dans le cadre d'une campagne de malware de cryptomining en cours

Des API Docker sur Des serveurs Linux ont été la cible d'une campagne de crypto minage de Monero à grande échelle menée par les opérateurs du botnet Lemon_Duck.

Les gangs de cryptomining constituent une menace constante pour les systèmes Docker mal sécurisés ou mal configurés. De nombreuses campagnes d'exploitation massive ont été signalées ces dernières années.

Une fois que la machine infectée est configurée pour le minage, Lemon_Duck tente un mouvement latéral en exploitant les clés SSH trouvées sur le système de fichiers. Si celles-ci sont disponibles, l'attaquant les utilise pour répéter le même processus d'infection.

Parallèlement à cette campagne, Cisco Talos en signale une autre, attribuée à TeamTNT, qui vise également les instances API Docker exposées sur Amazon Web Services.

Ce groupe de menaces tente également de désactiver les services de sécurité du cloud pour échapper à la détection et continuer à miner du Monero, du Bitcoin et de l'Ether aussi longtemps que possible.

Il est impératif de configurer les déploiements d'API Docker de manière sécurisée, et les administrateurs peuvent commencer par vérifier les meilleures pratiques et recommandations de sécurité de la plateforme par rapport à leur configuration.

En outre, il est recommandé de définir des limites de consommation de ressources sur tous les conteneurs, d'imposer des politiques strictes d'authentification des images et d'appliquer le principe du moindre privilège.

Source : https://bit.ly/3vGO7DX

Cloud… soyons prêts

Les tests post-migration

Après avoir terminé de tout migrer vers le cloud, il est important d'effectuer des tests post-migration afin d'assurer que la migration a été faite correctement. Ces tests concernent les trois éléments suivants :

1. Intégration : La réalisation de tests d'intégration après la migration des applications vers le cloud confirme que les applications se sont intégrées de manière transparente à la nouvelle infrastructure sous-jacente et aux autres applications tierces. Les tests d'intégration consistent à vérifier que les API et les bibliothèques fonctionnent toujours et que les dépendances entre les applications n'ont pas été rompues.

2. Sécurité : La sécurité est le facteur le plus important lors du stockage de données dans le cloud. La réalisation de divers tests, notamment des tests de pénétration, des audits de sécurité et des analyses de vulnérabilité sont nécessaire afin de confirmer que :

- Seuls les utilisateurs autorisés peuvent accéder à votre réseau en nuage ;
- Les mesures préventives contre les menaces courantes sont en place et fonctionnent correctement ;
- Les données en transit, en cours d'utilisation et au repos sont correctement sécurisées.

3. Performance : Le troisième élément qui permet de déterminer le succès de la migration des applications vers le cloud implique l'accès aux performances et aux temps de réponse. Cette étape importante permet de s'assurer que les clients et les utilisateurs finaux bénéficient toujours au moins des mêmes niveaux de performance qu'avant la migration.

Source : *https://bit.ly/38s44pP*

Bon à savoir !

Mon compte de messagerie a été piraté ! Que dois-je faire ?

Les comptes de messageries représentent est un véritable trésor car il y a de fortes chances qu'il contienne des années de correspondance avec vos amis et votre famille, ainsi que d'autres messages provenant de banques, de détaillants en ligne, de médecins, d'entrepreneurs, de contacts professionnels, etc. Dans l'ensemble, votre messagerie contient un grand nombre d'informations personnelles, ce qui en fait une cible de choix pour les pirates.

Si vous découvrez que votre messagerie a été piratée, ces cinq étapes peuvent vous aider à prévenir ou à minimiser les dommages causés :

1) Changez vos mots de passe : Changez le mot de passe de votre compte de messagerie si vous le pouvez. Faites-en un mot de passe fort et unique - ne réutilisez pas le mot de passe d'un autre compte. Ensuite, mettez à jour les mots de passe des autres comptes si vous utilisez le même ou un mot de passe similaire.

2) Utilisez le service de récupération de votre fournisseur de messagerie, si nécessaire : Dans le cas où votre compte est bloqué parce que vous pensez que le pirate a changé le mot de passe, votre fournisseur de messagerie doit pouvoir le récupérer. C'est une bonne raison de tenir à jour vos questions de sécurité et vos autres coordonnées auprès de votre fournisseur, car c'est le principal moyen de reprendre le contrôle de votre compte.

3) Contactez vos contacts de messagerie : Dès que vous le pouvez, envoyez un message à tous vos contacts de messagerie et faites-leur savoir que votre messagerie a été compromise. De même, prévenez-les qu'ils ne doivent pas ouvrir les e-mails ou les pièces jointes que vous avez envoyés pendant la période où votre compte a été compromis.

4) Recherchez les logiciels malveillants et les virus sur votre appareil : Il existe plusieurs façons pour un pirate de s'emparer des informations de votre compte de messagerie, notamment en utilisant des logiciels malveillants. Procédez à une analyse antivirus approfondie de votre appareil à l'aide d'un logiciel de protection complet pour vous assurer que votre appareil est exempt de logiciels malveillants. Si vous ne l'avez pas encore fait, configurez une analyse régulière à exécuter automatiquement. Cela vous aidera à garder les choses propres à long terme.

5) Vérifiez vos autres comptes : Parfois, un mauvais piratage en entraîne un autre. Si quelqu'un a accès à votre messagerie et à tous les messages qu'elle contient, il peut avoir ce dont il a besoin pour mener d'autres attaques. Jetez un coup d'œil à vos autres comptes bancaires, financiers, de médias sociaux et autres services que vous utilisez et gardez l'œil sur toute activité inhabituelle.

D'une manière plus générale, votre compte de messagerie électronique est l'une des nombreuses pièces qui composent le tableau d'ensemble de votre identité en ligne. Les autres éléments importants sont vos comptes bancaires en ligne, vos comptes d'achat en ligne, etc. Il ne fait aucun doute que vous devez garder un œil sur ces éléments.

Source : *https://bit.ly/3kbfP6u*

Evènements

Evènement du mois

Ne vous faites pas pirater !

27 Avril 2022, Online

https://bit.ly/3MAq8gw

Cet évènement a abordé les principales mesures à prendre pour se protéger en ligne, et la façon dont il faut réagir si les informations personnelles sont menacées. De plus, Digital Self-Defence Center, une nouvelle plateforme en ligne offrant une formation gratuite à la sécurité numérique pour les militants et les acteurs de la société civile a été présentée.

Evènement à venir

Introduction à la cybersécurité | Phishing pour les débutants |

20 Mai 2022, Online

https://bit.ly/3vPl5lx

Ce webinaire explique le principe de fonctionnement de phishing et la manière dont il a été utilisé dans de nombreuses attaques de cybersécurité, il décrit aussi comment faire face au phishing afin de se protéger contre ses cybercrimes.

Référence	ANPT-2022-BV-04
Titre	Bulletin de veille N°04
Date de version	30 Avril 2022
Contact	ssi@anpt.dz