BULLETIN DE VEILLE N°08

ANPT-2022-BV-08

"Cybersecurity is a new area where equality will exist to allow intelligence to succeed.
-- Ian R. McAndrew, PhD --

Août 2022

Alertes de sécurité

Kaspersky

Kaspersky corrige une faille d'élévation de privilèges locale dans VPN Secure Connection

04 Août 2022

Synopsys Cybersecurity Research Center a signalé une vulnérabilité de gravité élevée qui pourrait permettre une élévation de privilèges locale dans le VPN Secure Connection de Kaspersky pour Microsoft Windows.

Suivie sous le nom de CVE-2022-27535, la faille permettait à un attaquant authentifié de déclencher une suppression arbitraire de fichiers dans le système, cela pouvait entraîner un dysfonctionnement du dispositif ou la suppression de fichiers système importants nécessaires au bon fonctionnement du système.

L'équipe de Kaspersky a déclaré que pour exécuter cette attaque, un intrus devait créer un fichier spécifique et convaincre les utilisateurs d'exécuter les fonctionnalités du produit "Supprimer toutes les données de service et les rapports" ou "Enregistrer le rapport sur votre ordinateur".

La société a corrigé la faille dans la dernière version 21.6 de Kaspersky VPN Secure Connection et invite les utilisateurs de l'installer afin d'atténuer tout risque potentiel.

Source : *https://bit.ly/3AzH2Yr*

Cisco

Une faille critique d'exécution de code à distance dans les routeurs VPN de Cisco

03 Août 2022

Cisco a résolu des vulnérabilités de sécurité critiques ayant un impact sur les routeurs VPN Small Business et permettant à des attaquants distants non authentifiés d'exécuter du code ou des commandes arbitraires et de déclencher des conditions de déni de service (DoS) sur les appareils affectés.

Deux problèmes « CVE-2022-20842 et CVE-2022-20827 » ont été identifiés dans les interfaces de gestion Web et dans la fonction de mise à jour de la base de données des filtres Web, et sont tous deux causés par une validation insuffisante des entrées.

Une exploitation réussie de la première faille avec des entrées HTTP modifiées pourrait permettre aux attaquants d'exécuter un code arbitraire en tant qu'utilisateur root sur le système d'exploitation sous-jacent ou de provoquer le rechargement du dispositif, ce qui entraînerait une condition de déni de service.

Quant à la deuxième, elle consiste à transmettre des entrées falsifiées à la fonction de mise à jour de la base de données du filtre Web, peuvent permettre aux acteurs de la menace d'exécuter des commandes avec les privilèges de l'utilisateur root.

Les routeurs affectés par ces bogues comprennent les routeurs VPN de la série Small Business RV160, RV260, RV340 et RV345 (CVE-2022-20842 n'affecte que les deux derniers).

Cisco a également corrigé un troisième bug de haute gravité (CVE-2022-20841) dans le module Open Plug and Play (PnP) des routeurs des séries RV160, RV260, RV340 et RV345.

Il est recommandé de mettre à jour les systèmes concernés dès que possible pour éviter toute exploitation possible.

Source : *https://bit.ly/3AXor9Z*

Junkins

Jenkins : Bogues XSS et CSRF non corrigés dans le dernier avis des plugins

12 Juillet 2022

Un total de 27 vulnérabilités a été découvert dans la plateforme DevOps open source Jenkins affectant plus d'une douzaine de plugins, dont 5 ont été jugées comme ayant un impact "élevé" et dont la majorité n'est pas corrigée.

La première faille à fort impact est de type CSRF (cross-site request forgery), suivie sous le nom de CVE-2022-36920 affectant le plugin Coverity qui ne procède pas à une vérification des autorisations dans un point de terminaison HTTP. De plus, ce point de terminaison HTTP ne nécessite pas de requêtes POST, ce qui ouvre la porte aux attaques CSRF.

De plus, une vulnérabilité d'écriture de fichier arbitraire dans le CLIF Performance Testing Plugin (CVE-2022-36894) permet aux attaquants avec la permission 'Overall/Read' de créer ou de remplacer des fichiers arbitraires sur le système de fichiers du contrôleur Jenkins avec un contenu spécifié par l'attaquant.

Des failles XSS (cross-site scripting) stockées ont également été découvertes dans le plugin Dynamic Extended Choice Parameter (CVE-2022-36902) et le plugin Maven Metadata (CVE-2022-36905), ainsi qu'une vulnérabilité XSS réfléchie dans le plugin Lucene-Search (CVE-2022-36922).

"Notre recommandation aux administrateurs de Jenkins est de lire nos avis de sécurité pour comprendre s'ils sont impactés", a déclaré responsable de la sécurité de Jenkins. "Bien sûr, s'ils ne sont pas sûrs d'être affectés, la chose la plus sûre à faire est de désinstaller le plugin."

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

SAP

SAP corrige des vulnérabilités de haute gravité dans NetWeaver

15 Août 2022

Dans le cadre de son Security Patch Day de juin 2022, SAP a annoncé la publication de dix nouvelles notes de sécurité et de deux mises à jour.

Considérée comme " hautement prioritaire ", la plus grave des notes nouvellement publiées traite de CVE-2022-27668 (score CVSS de 8,6), un contrôle d'accès inapproprié lié au proxy SAProuter dans NetWeaver et ABAP Platform.

"Une configuration permissive de la table de permission des routes peut permettre à un attaquant non authentifié de contourner la protection pour exécuter des commandes d'administration sur les systèmes connectés au SAPRouter, compromettant ainsi la disponibilité des systèmes", explique la société de sécurité des applications d'entreprise Onapsis.

Une solution de contournement existe pour ce problème - impliquant le renforcement de la table de permission des routes et la suppression des caractères génériques des entrées de type 'P' et 'S'- mais il est conseillé aux clients d'appliquer le correctif disponible dès que possible.

Une autre faille de haute gravité (score CVSS de 8.2) a été corrigée qui peut conduire à la compromission du système.

Toutes les autres notes de sécurité nouvelles ou mises à jour annoncées cette semaine sont de "priorité moyenne" ou de "faible priorité".

Source : *https://bit.ly/3ABuj7k*

IBM

IBM corrige de graves failles dans le middleware de messagerie MQ

24 Août 2022

IBM a annoncé des correctifs pour des vulnérabilités de haute gravité dans IBM MQ (un middleware de messagerie et de mise en file d'attente), avertissant que des attaquants pourraient les exploiter pour contourner les restrictions de sécurité ou accéder à des informations sensibles.

Les deux bogues résolus se trouvaient dans la bibliothèque libcurl et pourraient être exploitées à distance.

Suivi sous le nom de CVE-2022-27780, le premier de ces bogues pourrait permettre à un attaquant de contourner les restrictions de sécurité en utilisant un nom d'hôte spécialement conçu dans une URL.

Le second problème, CVE-2022-30115, est dû à un contournement de la vérification HSTS et pourrait être exploité pour obtenir des informations sensibles via HTTP en clair.

Les versions 9.2 LTS, 9.1 LTS, 9.0 LTS, 9.2 CD et 9.1 CD d'IBM MQ se sont révélées vulnérables. Les deux vulnérabilités ont été corrigées dans le cadre de l'APAR IT40933.

IBM a également corrigé d'autres failles, une pourrait permettre à un acteur de la menace de provoquer une fuite d'informations dans le logiciel SANNav, et la deuxième est une vulnérabilité de déni de service trouvée dans Sterling Connect:Direct pour UNIX.

Il est recommandé de mettre à jour les systèmes concernés afin d'atténuer tout risque possible.

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

VMware

VMware incite les administrateurs à corriger un bogue critique de contournement d'authentification

02 Août 2022

VMware a corrigé une vulnérabilité critique de contournement d'authentification affectant les utilisateurs de domaine local dans plusieurs produits et permettant à des attaquants non authentifiés d'obtenir des privilèges d'administrateur.

Suivie sous le nom de CVE-2022-31656 avec un score de base CVSSv3 de 9,8, la faille a un impact sur VMware Workspace ONE Access, Identity Manager et vRealize Automation.

La société a également corrigé plusieurs autres bogues de sécurité permettant aux attaquants d'obtenir l'exécution de code à distance (CVE-2022-31658, CVE-2022-31659, CVE-2022-31665) et d'élever leurs privilèges jusqu'à " root " (CVE-2022-31660, CVE-2022-31661, CVE-2022-31664) sur les serveurs non patchés.

Selon Bob Plankers, architecte de la sécurité et de la conformité de l'infrastructure cloud chez VMware, il est extrêmement important de prendre rapidement des mesures pour corriger ou atténuer ces problèmes lors les déploiements sur site.

VMware a proposé une solution de contournement temporaire aux clients qui ne peuvent pas appliquer immédiatement le correctif CVE-2022-31656 à leurs systèmes.

Les étapes détaillées par VMware exigent que les administrateurs désactivent tous les utilisateurs à l'exception d'un administrateur provisionné et se connectent via SSH pour redémarrer le service horizon-workspace.

Cependant, VMware ne recommande pas l'utilisation de cette solution de contournement et indique que la seule façon de résoudre complètement la faille de contournement d'authentification CVE-2022-31656 est de patcher les produits vulnérables.

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

Actualité

Le réseau de Cisco a été compromis par un gang lié à Lapsus$

Cisco a révélé que des cybercriminels avaient accédé à son réseau d'entreprise en mai après que le compte Google personnel d'un employé ait été compromis.

La déclaration de Cisco affirme que l'entreprise "n'a pas identifié d'impact sur [ses] activités suite à cet incident, y compris sur les produits ou services Cisco, les données sensibles des clients ou les informations sensibles des employés, la propriété intellectuelle ou les opérations de la chaîne d'approvisionnement."

Cisco Security Incident Response (CSIRT) et le groupe intelligent de cybersécurité de l'entreprise, Cisco Talos, ont précisé que la seule exfiltration de données réussie provenait d'un compte avec le casier de stockage en nuage Box qui était associé au compte d'un employé compromis.

Selon l'article de Talos, l'attaquant a obtenu l'accès aux réseaux de Cisco, a inscrit une série de dispositifs pour l'AMF et s'est authentifié avec succès au VPN de Cisco.

L'infiltration s'est produite après que des attaquants ont volé les identifiants Cisco d'un employé en prenant le contrôle d'un compte Google personnel.

L'attaquant a ensuite employé des techniques de voice-phishing qui ont vu des agents appeler en se faisant passer pour diverses organisations de confiance, cherchant à aider l'employé de Cisco, jusqu'à ce qu'il craque et accepte une fausse notification MFA qui a donné aux pirates l'accès au VPN.

Une fois à l'intérieur, ils se sont propagés latéralement aux serveurs Citrix, pour finalement obtenir un accès privilégié aux contrôleurs de domaine. En tant qu'administrateurs de domaine, ils ont utilisé plusieurs outils pour exfiltrer des données et installer une porte dérobée et d'autres charges utiles.

Cisco a pu révoquer l'accès des attaquants, mais cela ne les a pas découragés. Ils ont tenté de se réinsérer à plusieurs reprises. Ils ont ensuite tenté d'établir une communication par courriel avec des cadres de Cisco, montrant des listes de répertoires de leur butin - 2,75 Go de données contenant environ 3 700 fichiers - et suggérant que Cisco pourrait payer pour éviter la divulgation.

"Sur la base des artefacts obtenus, des tactiques, techniques et procédures (TTP) identifiées, de l'infrastructure utilisée et d'une analyse approfondie de la porte dérobée utilisée dans cette attaque, nous estimons que cette attaque a été menée par un adversaire qui a été précédemment identifié comme un courtier d'accès initial (IAB) ayant des liens avec UNC2447 et Lapsus$ ", a déclaré Cisco, ajoutant que l'activité était également liée au gang de ransomware Yanluowang.

Il est intéressant de noter qu'aucun ransomware ne semble avoir été déployé dans l'attaque contre Cisco. « Bien que nous n'ayons pas observé le déploiement d'un ransomware lors de cette attaque, les TTP utilisées correspondaient à une "activité pré-ransomware", a déclaré Cisco.

La société a également révélé que la raison pour laquelle elle divulgue l'incident maintenant - plus de trois mois après la compromission - était qu'elle avait "activement collecté des informations sur le mauvais acteur pour aider à protéger la communauté de la sécurité". Mais une fois que les fichiers de l'incident ont été publiés sur le dark web, Cisco a estimé qu'elle devait révéler l'attaque.

Source : *https://bit.ly/3RgM4zF*

Le code source et les plans de LastPass ont été volés

Le fabricant de gestionnaires de mots de passe LastPass a déclaré que quelqu'un s'était introduit dans le compte d'un de ses développeurs et avait utilisé ce moyen pour accéder à des données exclusives.

La société a insisté sur le fait que les mots de passe de ses utilisateurs étaient toujours en sécurité, ajoutant que le vol a eu lieu il y a environ deux semaines. LastPass, propriété de GoTo, compterait plus de 25 millions d'utilisateurs et 80 000 entreprises clientes.

"Nous avons déterminé qu'une partie non autorisée a eu accès à des portions de l'environnement de développement de LastPass par le biais d'un seul compte de développeur compromis et a pris des portions du code source et certaines informations techniques exclusives de LastPass", a déclaré le PDG Karim Toubba dans un communiqué.

Toubba a ajouté : « Après avoir lancé une enquête immédiate, nous n'avons vu aucune preuve que cet incident impliquait un accès aux données des clients ou aux coffres de mots de passe cryptés. »

L'effraction est apparue, nous dit-on, après qu'une "activité inhabituelle" a été détectée dans la zone de développement du réseau informatique de LastPass. L'éditeur de logiciels a déclaré qu'il avait contenu la faille de sécurité, pris des mesures pour éviter qu'elle ne se reproduise et contacté des experts en sécurité informatique externes pour obtenir de l'aide.

"Notre enquête n'a montré aucune preuve d'un accès non autorisé aux données des clients dans notre environnement de production", a ajouté LastPass dans un communiqué. "Pour l'instant, nous ne recommandons aucune action de la part de nos utilisateurs ou administrateurs."

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

Des employés de Microsoft ont exposé les logins internes

Plusieurs employés de Microsoft ont exposé des identifiants de connexion sensibles à la propre infrastructure de l'entreprise sur GitHub, offrant aux attaquants une passerelle vers les systèmes internes de Microsoft.

"Nous continuons à voir que les fuites accidentelles de code source et d'informations d'identification font partie de la surface d'attaque d'une entreprise, et il devient de plus en plus difficile de les identifier de manière opportune et précise. C'est un problème très difficile pour la plupart des entreprises de nos jours", a déclaré Mossab Hussein, responsable de la sécurité

chez la société de cybersécurité SpiderSilk, qui a découvert le problème, lors d'une discussion en ligne avec Motherboard.

Hussein a fourni à Motherboard sept exemples au total d'identifiants Microsoft exposés. Tous ces exemples étaient des identifiants pour des serveurs Azure. Trois des sept identifiants de connexion étaient encore actifs lorsque SpiderSilk les a découverts.

En ce qui concerne la nouvelle exposition des informations d'identification, un porte-parole de Microsoft a déclaré à Motherboard dans un courriel que "Nous avons enquêté et pris des mesures pour sécuriser ces informations d'identification. Bien qu'elles aient été rendues publiques par inadvertance, nous n'avons vu aucune preuve que des données sensibles aient été accédées ou que les informations d'identification aient été utilisées de manière inappropriée. Nous poursuivons notre enquête et continuerons à prendre les mesures nécessaires pour empêcher davantage le partage par inadvertance des informations d'identification."

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

VirusTotal révèle les logiciels les plus usurpés dans les attaques de malware

Les acteurs de la menace imitent de plus en plus des applications légitimes comme Skype, Adobe Reader et VLC Player afin d'abuser des relations de confiance et d'augmenter la probabilité de réussite d'une attaque d'ingénierie sociale.

Parmi les autres applications légitimes les plus imitées par icône figurent 7-Zip, TeamViewer, CCleaner, Microsoft Edge, Steam, Zoom et WhatsApp, selon une analyse de VirusTotal.

Les acteurs de la menace aient recours à diverses approches pour compromettre les points finaux en incitant les utilisateurs non avertis à télécharger et à exécuter des exécutables apparemment inoffensifs. Pour ce faire, ils tirent parti de domaines authentiques afin de contourner les défenses des pare-feu basés sur l'IP. Parmi les domaines les plus exploités figurent discordapp[.]com, squarespace[.]com, amazonaws[.]com, mediafire[.]com et qq[.]com.

Une autre technique souvent utilisée consiste à signer les logiciels malveillants avec des certificats valides volés à d'autres fabricants de logiciels.

VirusTotal a également découvert 1 816 échantillons depuis janvier 2020 qui se faisaient passer pour des logiciels légitimes en intégrant le malware dans des programmes d'installation d'autres logiciels populaires tels que Google Chrome, Malwarebytes, Zoom, Brave, Mozilla Firefox et Proton VPN.

Cette méthode de distribution peut également donner lieu à une attaque de la chaîne d'approvisionnement lorsque des adversaires parviennent à s'introduire dans le serveur de mise à jour d'un logiciel légitime ou à obtenir un accès non autorisé au code source, ce qui permet de glisser le malware sous la forme de binaires trojanisés.

"Si l'on considère ces techniques dans leur ensemble, on peut conclure qu'il existe à la fois des facteurs opportunistes dont les attaquants peuvent abuser (comme des certificats volés) à court et à moyen terme, et des procédures automatisées de routine (très probablement) dans lesquelles les attaquants visent à reproduire visuellement des applications de différentes manières", ont déclaré les chercheurs.

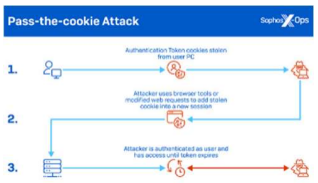
Source : *https://bit.ly/3TnXQtZ*

Exploitation de cookies de session volés pour contourner l'authentification multi-facteurs (MFA)

Selon Sophos, les attaquants exploitent de plus en plus les cookies de session volés pour contourner l'authentification multifactorielle (MFA) et accéder aux ressources de l'entreprise.

Dans deux des incidents récents sur lesquels Sophos a enquêté, les attaquants ont adopté une approche ciblée. Dans un cas, les attaquants ont passé des mois à l'intérieur du réseau d'une cible à recueillir des cookies du navigateur Microsoft Edge.

Dans un autre cas, les attaquants ont utilisé un composant légitime de Microsoft Visual Studio pour déposer une charge utile malveillante qui a récupéré des fichiers de cookies pendant une semaine.



" Étant donné qu'une grande partie du lieu de travail est désormais basée sur le Web, il n'y a vraiment pas de limite aux types d'activités malveillantes que les attaquants peuvent mener avec des cookies de session volés. Ils peuvent altérer les infrastructures en nuage, compromettre la messagerie professionnelle, convaincre d'autres employés de télécharger des logiciels malveillants ou même réécrire le code de produits. La seule limite est leur propre créativité", a déclaré M. Gallagher.

"Ce qui complique les choses, c'est qu'il n'y a pas de solution facile. Par exemple, les services peuvent raccourcir la durée de vie des cookies, mais cela signifie que les utilisateurs doivent se réauthentifier plus souvent, et, comme les attaquants se tournent vers des applications légitimes pour gratter les cookies, les entreprises doivent combiner la détection des logiciels malveillants avec l'analyse comportementale."

Source : *https://bit.ly/3KuU6*

Bon à savoir

Les cinq meilleures pratiques en matière de gestion des correctifs

Aujourd'hui, avec l'augmentation excessive de vulnérabilités et donc les correctifs correspondants, les entreprises sont inondées par le nombre de correctifs à traiter. C'est pourquoi les organisations ne peuvent pas négliger l'importance cruciale d'une bonne pratique de gestion des correctifs

Les cinq meilleures pratiques de gestion des correctifs suivantes peuvent aider les entreprises à créer un programme de défense solide contre l'exploitation des vulnérabilités.

1. Identifier les correctifs les plus pertinents : Les organisations devraient commencer par se concentrer uniquement sur les bogues pertinents pour les systèmes d'application qu'elles utilisent en interne. À partir de là, les équipes de sécurité peuvent s'efforcer de déterminer lesquels de ces bogues sont activement exploités et lesquels font partie de l'infrastructure critique de l'entreprise. L'étape suivante consiste à identifier les applications et/ou les systèmes d'exploitation qui ont activement exploité des vulnérabilités dans la nature ainsi que les vulnérabilités qui ont fait l'objet d'une démonstration de faisabilité (POC).

2. Préparer un plan pour les "zero-day" : Il est difficile de se défendre contre les failles de type "zero day" en raison de leur nature même. Une surveillance constante des activités suspectes au sein des réseaux est indispensable pour se défendre contre ce type d'exploits. Rester à jour avec les programmes de primes aux bugs, est un moyen idéal de les surveiller et d'avoir un aperçu des correctifs publics pour les corriger.

3. Communiquer avec les fournisseurs : Aujourd'hui, les organisations peuvent investir dans des versions SaaS des applications, ce qui signifie que les fournisseurs peuvent appliquer automatiquement des correctifs et des mises à jour aux logiciels sans avoir à intervenir ou à obtenir une autorisation. Cependant, parfois même un bon correctif peut mettre temporairement un système hors service. Pour éviter les problèmes potentiels liés aux correctifs automatisés, les entreprises doivent communiquer avec leurs fournisseurs sur la possibilité de revenir à des versions antérieures des logiciels.

4. Utiliser le correctif virtuel : Contrairement au correctif manuel, le correctif virtuel est une mise en œuvre à court terme des correctifs réels apportés aux vulnérabilités connues. Ils peuvent être appliqués sans avoir à redémarrer les systèmes, ce qui en fait d'excellents substituts provisoires en attendant qu'un correctif du fournisseur soit publié.

5. Partager les avantages avec les parties prenantes : Un programme de cybersécurité n'a de force que si l'organisation y croit. Lorsqu'il s'agit de communiquer avec les parties prenantes sur la gestion des correctifs, l'accent est mis sur le risque. Les vulnérabilités exploitées ont une chance extrêmement élevée de compromettre le risque. Comme les entreprises continuent d'étendre leurs empreintes avec plus de logiciels et de matériel, le potentiel d'une attaque malveillante augmentera également.

La cybersécurité représente un investissement important, mais le coût de l'absence d'investissement est encore plus élevé. Les exploitations de vulnérabilités continueront d'augmenter chaque année. Les entreprises doivent donc se concentrer sur le développement d'une stratégie de gestion des correctifs afin d'établir une base solide pour leurs pratiques de cybersécurité, ce qui leur permettra de passer au niveau supérieur.

Source : *https://bit.ly/3R2GRMi*

Evènements

Evènement du mois

Attack and Defense : Protecting the Cloud

30 Août 2022

Online

https://bit.ly/3RnKJJ5

Cet évènement aborde le thème de la sécurité les données stockées dans le cloud. Les principaux points abordés sont :

- Comprendre comment les attaquants peuvent compromettre un cloud.
- Identifier les stratégies de défense qui peuvent être prises pour réduire les risques potentiels.
- Prendre les bonnes mesures pour bien protéger les données et le structure de cloud.

Evènement à venir

Intro to Cybersecurity Certifications : Workshop

22 Septembre 2022

Online

https://bit.ly/3wHAEwZ

Cet évènement vise à expliquer comment les certifications en cybersécurité participent pour valider les compétences acquises d'une manière reconnue par le secteur.

Au cours de ce séminaire destiné aux nouveaux arrivants dans le domaine de la cybersécurité, l'équipe de la Flatiron School va expliquer les points suivants :

- Faut-il une certification pour obtenir un emploi dans la cybersécurité ?
- Comment les certifications peuvent aider à développer une carrière personnelle ?
- Comment identifier la certification qui correspond à ses objectifs voulus.

Référence	ANPT-2022-BV-08
Titre	Bulletin de veille N°08
Date de version	31 Août 2022
Contact	ssi@anpt.dz