BULLETIN DE VEILLE N°02

ANPT-2022-BV-02

"You are an essential ingredient in our ongoing effort to reduce Security Risk."
-- Kirsten Manthorne --

Février 2022

Alertes de sécurité

Microsoft

Patch Tuesday corrige 48 failles dont une Zero-day

08 février 2022

Avec la publication de Patch Tuesday de février 2022, Microsoft a corrigé une vulnérabilité zero-day et un total de 48 failles (sans compter 22 vulnérabilités de Microsoft Edge), mais aucune d'entre elles n'est classée comme critique.

Parmi les vulnérabilités corrigées, on trouve 16 d'élévation de privilèges, 3 liées au contournement des fonctionnalités de sécurité, 16 d'exécution de code à distance, 5 liées à la divulgation d'informations, 5 DoS et 3 d'usurpation d'identité.

La faille de type zero-day corrigée, nommée CVE-2022-21989, est une vulnérabilité d'élévation de privilèges dans le noyau Windows avec un score CVSS 7.8/10. Ce bogue est publié mais n'est pas encore exploité par les acteurs de menace.

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

SAP

De graves vulnérabilités de contrebande ont été corrigées dans les produits SAP

08 Février 2022

SAP a publiée des correctifs pour 22 vulnérabilités dont certaines qui sont extrêmement critiques affectant les applications SAP basées sur SAP NetWeaver.
Suivies sous le nom CVE-2022-22536 et CVE-2022-22532, ces failles permettent à un attaquant non authentifié d'accéder à distance à une application SAP affectée et d'obtenir un contrôle total du système,
Les autres failles trouvées dans le même produit sont :

- CVE-2022-22540 : Vulnérabilité d'injection SQL ;
- CVE-2022-22534 : Vulnérabilité XSS ;
- CVE-2022-22545 : Vulnérabilité de divulgation d'informations ;
- CVE-2022-22543 : Vulnérabilité de déni de service DoS.

La plupart des corrections classées comme HotNews (gravité maximale) résolvent la faille Log4j trouvée dans les applications SAP (SAP Commerce, SAP Data Intelligence 3, SAP Dynamic Authorization Management, SAP Customer Checkout, etc.).
Toutes ces vulnérabilités permettent aux acteurs de la menace à distance d'exécuter du code sur des systèmes exécutant des logiciels non corrigés après une exploitation réussie.

Source : *https://bit.ly/3h797Nk*

Siemens

Les vulnérabilités du BIOS Insyde infectent les produits industriels Siemens

22 Février 2022

Multiples vulnérabilités ont été trouvées dans le BIOS Insyde qui est utilisé par les produits « Siemens Industry ». Ces failles permettent à un acteur de menace de provoquer une exécution de code arbitraire à distance et une élévation de privilèges.
Le produit Siemens affecté par ces vulnérabilités est le dispositif de programmation mobile et standard pour les ingénieurs en automatisation « SIMATIC Field PG ». Parmi ces vulnérabilités, il y a :

• CVE-2022-24030, CVE-2022-24031 : Deux vulnérabilités de corruption de mémoire SMM dans InsydeH2O, la première est trouvée dans le composant AhciBusDxe et la deuxième dans NvmExpressDxe. Ces deux bogues peuvent permettre à un attaquant d'écrire des données fixes ou prévisibles dans SMRAM. L'exploitation de ce problème pourrait entraîner une escalade des privilèges vers SMM.
• CVE-2022-24069 : Une vulnérabilité de légende SMM permet à un attaquant de détourner le flux d'exécution de code exécuté en mode de gestion du système. L'exploitation de ce problème pourrait entraîner une escalade des privilèges vers SMM.
Afin d'atténuer tout risque possible, Siemens recommande vivement de protéger l'accès au réseau des appareils par des mécanismes appropriés et de limiter les possibilités d'exécution d'un code non fiable.

Source : *https://sie.ag/3sqjq5D*

Cisco

Une vulnérabilité DoS dans plusieurs produits Cisco

04 Février 2022

Cisco a publié des mises à jour qui corrigent une vulnérabilité de haute gravité dans le préprocesseur Modbus (Un protocole de communication utilisé pour des réseaux d'automates programmables) du moteur de détection Snort, qui pourrait permettre à un acteur de menace distant non authentifié de causer un déni de service sur le périphérique affecté.

Connue sous le nom CVE-2022-20685 avec un score de 7.5 sur l'échelle CVSS, cette faille est provoquée par un débordement d'entier lors du traitement du trafic Modbus. Un attaquant peut exploiter cette vulnérabilité pour bloquer le processus Snort, entraînant l'arrêt de l'inspection du trafic.
Il est recommandé d'appliquer ces mises à jour afin de se protéger.

Source : *https://bit.ly/33JRMah*

Vulnérabilité d'injection de commandes logicielles dans Cisco IOS XE SD-WAN

17 Février 2022

Une vulnérabilité de haute gravité a été découverte dans l'interface de ligne de commande du logiciel Cisco IOS XE SD-WAN qui pourrait permettre à un attaquant local authentifié d'exécuter des commandes arbitraires avec des privilèges root.

Suivie sous le nom CVE-2021-1529, cette faille peut être exploitée en s'authentifiant auprès d'un appareil affecté et en soumettant des données modifiées à l'interface CLI du système.

Les produits affectés par ce problème sont :

• Routeurs à intégration de services (ISR) série 1000 et série 4000 ;

• Routeurs de services d'agrégation ASR série 1000 ;

• Plates-formes Edge de la série Catalyst 8000 ;

• Routeur de services cloud (CSR) série 1000V.

Cisco recommande ses clients de mettre à jour leurs logicielles vers des versions corrigées.

Source : *https://bit.ly/3seRod4*

IBM

Plusieurs vulnérabilités dans IBM HTTP Server

25 Février 2022

De nombreuses vulnérabilités existent dans la bibliothèque « Expat », qui affecte « IBM HTTP Server » utilisé par IBM WebSphere Application Server.

Dix failles ont affecté le serveur HTTP d'IBM, permettant ainsi à un acteur de menace de provoquer une exécution de code arbitraire à distance et un déni de service.

Les vulnérabilités les plus importantes sont :

- CVE-2021-45960 : Vulnérabilité DoS causée par un problème de comportement de réallocation dans la fonction storeAtts de xmlparse.c ;
- CVE-2022-22822, CVE-2022-23990, CVE-2022-23852 : Vulnérabilités RCE en raison d'un dépassement d'entier dans plusieurs fonctions.

IBM recommande vivement de corriger ces vulnérabilités le plus tôt possible en appliquant le correctif provisoire ou le groupe de correctifs actuellement disponible dans son site web.

Source : *https://ibm.co/3spRq1T*

Okta

Un nouveau bogue dans Okta client de type « RCE »

25 Février 2022

Une nouvelle mise à jour de sécurité a été publiée pour corriger une vulnérabilité d'exécution de code à distance dans le client Windows pour la plate-forme de gestion de l'authentification Okta Advanced Server Access.

Okta Advanced Server Access fournit une gestion des identités et des accès Zero Trust pour l'infrastructure cloud et locale. Il gère l'accès SSH et RDP aux serveurs Linux et Windows.

La faille identifiée sous le nom CVE-2022-24295, permet à des attaquants distants d'effectuer une injection de commande via une URL spécialement conçue. Ce type d'attaque « RCE » peut conduire à un contrôle complet du système, à une exfiltration silencieuse de données, à un déplacement latéral du réseau et à un accès initial aux réseaux d'entreprise.

Toutes les versions antérieures à 1.57.0 d'Okta Advanced Server Access Client pour Windows ont été infectées par cette vulnérabilité. De ce fait, il est recommandé de mettre à jour les systèmes affectés afin d'atténuer les menaces possibles.

Source : *https://bit.ly/3vrP7NM*

GE Digital

Deux vulnérabilités dans les produits GE SCADA

25 Février 2022

GE Digital a publié des correctifs et des mesures d'atténuation pour deux vulnérabilités de haute gravité affectant son logiciel « Proficy CIMPLICITY HMI/SCADA », qui est utilisé par des usines du monde entier pour surveiller et contrôler les opérations.

L'une de ces failles, répertoriée sous le nom de CVE-2022-23921, peut permettre à un attaquant ayant un accès limité au serveur « CIMPLICITY » d'élever ses privilèges en déposant un fichier malveillant dans le projet d'exécution « CIMPLICITY ».

Le deuxième problème, identifié comme CVE-2022-21798, est lié à la transmission d'informations d'identification en texte clair. Un attaquant qui peut capturer les informations d'identification par une attaque de type "man-in-the-middle" (MitM) peut les utiliser pour s'authentifier auprès de l'IHM et obtenir des informations sur les alertes et d'autres parties du système. GE a déclaré qu'un attaquant peut également, dans certains cas, être en mesure de modifier les valeurs du système.

Les deux vulnérabilités ont été corrigées par la mise à jour publiée par GE.

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

Actualité

Une nouvelle technique de phishing permettant de contourner l'authentification multifactorielle !

Le chercheur mr.d0x a découvert une nouvelle technique de hameçonnage qui permet de contourner l'authentification multifactorielle (MFA) en utilisant le logiciel d'accès à distance noVNC et les navigateurs fonctionnant en mode kiosque.

"Comment utiliser noVNC pour voler des informations d'identification et contourner le système 2FA ? Configurez un serveur avec noVNC, exécutez Firefox (ou tout autre navigateur) en mode kiosque et dirigez-vous vers le site Web sur lequel vous souhaitez que l'utilisateur s'authentifie (par exemple accounts.google.com)", explique un rapport de mr.d0x sur sa nouvelle technique de phishing.

"Envoyez le lien à l'utilisateur cible et lorsque celui-ci clique sur l'URL, il accède à la session VNC sans s'en rendre compte. Et comme vous avez déjà configuré Firefox en mode kiosque, tout ce que l'utilisateur verra est une page Web, comme prévu."

Grâce à cette configuration, un acteur de menace peut envoyer des e-mails de spear-phishing ciblés contenant des liens qui lancent automatiquement le navigateur de la cible et la connectent au serveur VNC distant de l'attaquant.

Comme le serveur VNC de l'attaquant est configuré pour exécuter un navigateur en mode kiosque, ce qui fait fonctionner le navigateur en mode plein écran, lorsque la victime clique sur un lien, elle verra simplement un écran de connexion pour le service de messagerie ciblé et se connectera normalement.

Cependant, comme l'invite de connexion est affichée par le serveur VNC de l'attaquant, toutes les tentatives de connexion se feront directement sur le serveur distant, mr.d0x a expliqué, qu'une fois l'utilisateur est connecté au compte, l'attaquant peut utiliser divers outils pour voler les informations d'identification et les jetons de sécurité.

Plus dangereux encore, cette technique contournera le MFA puisque l'utilisateur saisira le code d'accès à usage unique directement sur le serveur de l'attaquant, autorisant l'appareil pour les futures tentatives de connexion.

Pour ce qui est de la manière de se protéger contre ce type d'attaques, tous les conseils en matière de phishing restent les mêmes : ne pas cliquer sur les URL provenant d'expéditeurs inconnus, vérifier que les liens intégrés ne contiennent pas de domaines inhabituels et traiter tous les messages électroniques comme suspects, en particulier lorsqu'ils invitent à des connexion aux différents comptes.

***Source** : https://bit.ly/36MO00Y*

Des pirates informatiques déposent des fichiers exécutables malveillants dans les conversations Teams

Les chercheurs en cybersécurité de la société de sécurité Avanan ont détecté que certains acteurs de la menace ciblent Microsoft Teams pour placer des documents malveillants dans les fils de discussion, qui mettent généralement en œuvre des chevaux de Troie, en raison de sa popularité.

Les analystes affirment que les attaquants volent les informations d'identification des e-mails par le biais du phishing ou en négociant avec des organisations associées.

De nombreux utilisateurs ont fait confiance aux fichiers qu'ils ont reçus par le biais de Teams, et nous pouvons donc dire que c'est assez efficace.

Afin de se défendre contre ce type d'attaques, l'analyste de sécurité d'Avanan a recommandé de mettre en place une protection qui téléchargera tous les fichiers dans un bac à sable et vérifiera ensuite le contenu malveillant, de déployer une sécurité robuste à plein temps, car elle assurera toutes les lignes de communication de l'entreprise, ce qui inclut également Teams, et enfin, d'inciter les utilisateurs finaux à contacter le service informatique s'ils voient un fichier inconnu.

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

Un wiper malwar utilisé dans des cyberattaques destructrices contre l'Ukraine

Selon Symantec, le malware HermeticWipe a été utilisé dans certaines des récentes cyberattaques visant à effacer des données contre des organisations en Ukraine.

Une fois exécuté, le wiper ajuste ses paramètres pour obtenir le contrôle d'accès en lecture à n'importe quel fichier, puis obtient les privilèges nécessaires pour charger et décharger les pilotes de périphériques, désactive les vidages de pannes pour couvrir ses traces, désactive le Volume Shadow Service (VSS) et charge un gestionnaire de partition bénin dont il abuse pour corrompre le MBR.

Il utilise différentes méthodes de corruption en fonction de la version de Windows exécutée sur la machine et du type de partition (FAT ou NTFS). HermeticWiper peut endommager les disques MBR et GPT et déclenche un redémarrage du système pour achever le processus de suppression des données, notent les chercheurs de la division Talos de Cisco.

La société de cybersécurité a également trouvé des preuves que le wiper a été utilisé dans des attaques contre des ordinateurs en Lituanie également.

Dans les deux attaques, les acteurs de la menace à l'origine du wiper ont volé des informations d'identification trouvées dans les environnements compromis et ont exécuté le wiper à l'aide de tâches planifiées.

À l'instar des cyberattaques WhisperGate en Ukraine, certains des incidents HermeticWiper impliquaient l'exécution d'un ransomware sur les machines infectées. Cependant, Symantec

pense que le ransomware n'a été utilisé que pour détourner l'attention des attaques destructrices par effacement de données.

IBM et Symantec préviennent que l'évolution de la situation en Ukraine devrait s'accompagner de cyberattaques plus destructrices, susceptibles de s'intensifier parallèlement au conflit en cours.

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

Nvidia enquête sur une éventuelle cyberattaque

Le géant américain des puces Nvidia a confirmé qu'il enquêtait actuellement sur un "incident" qui aurait mis hors service certains de ses systèmes pendant deux jours.

Les systèmes touchés par ce qui semble être une cyberattaque comprennent les outils de développement et les systèmes de messagerie de l'entreprise, comme l'a rapporté The Telegraph.

La panne signalée est le résultat d'une intrusion dans le réseau, et on ne sait pas encore si des données d'entreprise ou de clients ont été volées pendant l'incident.

"Nous travaillons toujours à évaluer la nature et la portée de l'événement et n'avons pas d'informations supplémentaires à partager pour le moment." a déclaré Nvidia.

Un initié a décrit cet incident comme ayant "complètement compromis" les systèmes internes de Nvidia.

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

Le guide de la NSA sur les mots de passe des appareils Cisco

La National Security Agency (NSA) a publié des recommandations concernant l'utilisation de mots de passe spécifiques pour sécuriser les appareils Cisco.

"Chaque appareil possède des fichiers de configuration en clair qui contiennent des paramètres contrôlant le comportement de l'appareil, déterminant comment diriger le trafic réseau, et stockant les clés pré-partagées et les informations d'authentification des utilisateurs. Toutes les informations d'identification contenues dans les fichiers de configuration de Cisco risquent d'être compromises si des mots de passe forts ne sont pas utilisés", indique la NSA.

Pour aider les administrateurs à mieux sécuriser leurs environnements, l'agence a publié le guide Cisco Password Types : Best Practices, qui explique la difficulté de craquer les différents types de protection par mot de passe sur les appareils Cisco et la facilité avec laquelle il est possible de récupérer le mot de passe en clair dans certains cas.

Sur la base de l'analyse des différents types de protection des mots de passe Cisco, l'agence recommande l'utilisation de mots de passe de type 8 uniquement, et déconseille fortement l'utilisation de mots de passe de type 0 (aucun chiffrement ou hachage n'est utilisé), 4 (ils contiennent une erreur d'implémentation qui le rend faible face aux tentatives de brute force) et 7 (qui sont stockés sous forme de chaînes codées et doivent être considérés comme obfusqués, plutôt que chiffrés).

En outre, les mots de passe de type 8 offrent une protection solide, sans qu'aucun problème n'ait été constaté à leur sujet, indique la NSA. Les mots de passe sont hachés en utilisant PBKDF2, SHA-256, un sel de 80 bits et 20 000 itérations, et sont stockés sous forme de hachages dans les fichiers de configuration.

Il est aussi conseillé aux administrateurs d'utiliser des mots de passe longs et complexes pour accéder au mode EXEC et d'appliquer le principe du moindre privilège pour les différents comptes utilisateurs.

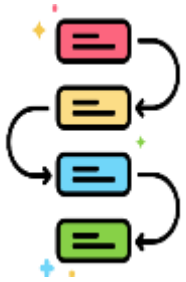
Source : *https://bit.ly/3vsSa8F*

Cloud… soyons prêts

La création d'un plan migration vers le cloud

La migration des données est un processus complexe, qui commence par l'évaluation des actifs de données existants et la conception d'un plan de migration. La phase de planification peut être divisée en quatre étapes.

1. Affiner le champ d'application en filtrant toutes les données excédentaires et en définissant la plus petite quantité d'informations nécessaire pour faire fonctionner le système efficacement. Il est possible d'effectuer une analyse de haut niveau des systèmes source et cible, en consultation avec les utilisateurs de données qui seront directement touchés par les changements à venir.
2. Evaluer les systèmes source et cible. Un plan de migration doit comprendre une évaluation approfondie des exigences opérationnelles du système actuel et de la manière dont elles peuvent être adaptées au nouvel environnement.
3. Définir des normes de données. Cela permettra de repérer les zones problématiques à chaque phase du processus de migration et d'éviter les problèmes inattendus au stade de la post-migration.
4. Une fois le périmètre affiné et les systèmes évalués, il est plus facile de choisir, d'estimer les ressources nécessaires au projet, de fixer des calendriers et des délais. Selon les estimations d'Oracle, un projet de migration de données à l'échelle d'une entreprise dure en moyenne de six mois à deux ans.



Sources : *https://bit.ly/3K3wdRh*

Bon à savoir !

Pourquoi la formation à la sensibilisation à la sécurité est-elle encore si importante aujourd'hui ?

1. Prévenir les violations et les attaques : Selon l'entreprise CyberSafe, en 2019, l'erreur humaine était à l'origine de 90 % des brèches. La formation à la sensibilisation à la sécurité permet de minimiser considérablement le taux de violation.

2. Construire une culture de la sécurité : Créer une culture de la sécurité signifie intégrer les valeurs de la sécurité dans le tissu de votre entreprise. Une formation qui couvre la sensibilisation à la situation, ainsi que les avantages liés au travail et à la vie privée, est un bon moyen de faire adhérer les gens.

3. Rendre les défenses technologiques plus robustes : Aujourd'hui, peu d'entreprises rêveraient de fonctionner sans défenses technologiques. Et pourtant, sans formation de sensibilisation à la sécurité, les défenses technologiques ne peuvent pas réaliser leur potentiel, vu que les attaquants ciblent généralement les personnes, car elles sont considérées comme un moyen facile d'accéder aux réseaux protégés.

4. Pour donner confiance à vos clients : Une entreprise qui prend des mesures pour améliorer la cybersécurité sera mieux à même de susciter la confiance des consommateurs. Et une entreprise de confiance est une entreprise à laquelle les clients restent fidèles.

5. Pour la conformité : La conformité peut être un heureux sous-produit de la formation à la sensibilisation à la sécurité. Ceux qui l'introduisent deviennent plus sûrs et, dans de nombreux secteurs, répondent aux exigences réglementaires.

6. Être socialement responsable en tant qu'entreprise : Comme WannaCry et NotPetya l'ont démontré en 2017, les cyberattaques peuvent se propager à grande vitesse. Plus il y a de réseaux infectés, plus les autres réseaux deviennent à risque. Et la faiblesse d'un réseau augmente la menace globale pour les autres.

7. Améliorer le bien-être des employés : Il est bien connu que les personnes heureuses sont des personnes productives. Il est donc utile de rappeler que la formation à la sensibilisation à la sécurité ne garantit pas seulement la sécurité des employés au travail. Elle les protège également leur vie privée.

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

Evènements

Evènement du mois

Micro Club Capture The Flag

26 Février 2022

Palais de la Culture Moufdi Zakaria, Alger, *Algérie*

https://bit.ly/3C0Dv5B

Micro Club Capture The Flag est l'événement qui a rassemblé les personnes passionnées et intéressées par la cybersécurité,

L'évènement a proposé de nombreuses activités (conférences, Talks, Workshops et CTF) traitant plusieurs thématiques comme :

- RED TEAMING POUR ANTICIPER LES FUTURES ATTAQUES ;
- SOCIAL ENGINEERING: HACK THE HUMANS;
- NEXT GENERATION SECURITY OPERATIONS CENTERS;
- HOW TO START YOUR PENTESTING CAREER.

Evènement à venir

ICT MAGHREB

14 au 16 Mars 2022

Palais de la Culture Moufdi Zakaria, Alger, *Algérie*

https://bit.ly/3soVtvo

ICT MAGHREB 2022 est une exposition professionnelle des technologies de l'information et de la communication destinée aux responsables IT. L'évènement se déroulera au Palais de la Culture Moufdi Zakaria, accueillera plus de 5.000 visiteurs professionnels et 150 exposants dont les principaux acteurs algériens du secteur des Technologies de l'Information ainsi que 40% d'entreprises étrangères parmi lesquelles les grandes multinationales. Plus de 40 conférenciers, exposés, conférences, débats et ateliers sont programmés sur 3 jours.

Référence	ANPT-2022-BV-02
Titre	Bulletin de veille N°02
Date de version	28 Février 2022
Contact	ssi@anpt.dz