BULLETIN DE VEILLE N°01

ANPT-2022-BV-01

"The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: Cybersecurity is much more than an IT topic"

-Srephane Nappo-

Janvier 2022

Alertes de sécurité

Microsoft

Patch Tuesday: Microsoft corrige97 vulnérabilités dont 6 zero-days

11 Janvier 2022

Microsoft a corrigé 97 vulnérabilités (plus 29 vulnérabilités de Microsoft Edge) dans le patch Tuesday de ce mois, dont neuf sont classées comme critiques et 88 comme importantes. Parmi ces vulnérabilités, il y a celles d'élévation de privilège, de contournement des fonctions de sécurité, d'exécution de code à distance, la divulgation d'informations, etc.

Ce patch aussi comprend des correctifs pour six vulnérabilités de type "zero-day" divulguées publiquement et non exploitées dans des attaques, qui portent les noms suivants :

- CVE-2021-22947 : Exécution de code à distance dans Curl Open Source ;
- CVE-2021-36976 : Exécution de code à distance dans Libarchive ;
- CVE-2022-21919 : Elévation de privilèges dans le service de profil utilisateur Windows ;
- CVE-2022-21836 : Usurpation de certificat Windows ;
- CVE-2022-21839 : Déni de service liée à la liste de contrôle d'accès discrétionnaire du suivi des événements Windows ;
- CVE-2022-21874 : Exécution de code à distance dans l'API du Centre de sécurité Windows.

Source: *https://bit.ly/3fU6ttD*

Des correctifs d'urgence pour Windows Server

17 Janvier 2022

Microsoft a publié une mise à jour hors bande d'urgence (OOB) pour Windows Server qui corrige de nombreux bogues critiques introduits lors du Patch Tuesday de janvier 2022.
Après avoir installé les mises à jour de janvier 2022, les administrateurs Windows server ont commencé à signaler des problèmes graves, notamment des contrôleurs de domaine entrant dans des boucles de démarrage, Hyper-V ne démarrant plus, des connexions VPN L2TP défaillantes et des volumes ReFS devenant inaccessibles.
Les problèmes étaient suffisamment graves pour que de nombreux administrateurs choisissent de désinstaller les mises à jour et de renoncer aux correctifs de sécurité inclus afin que leurs serveurs puissent fonctionner correctement à nouveau.
Microsoft a enfin publié des mises à jour avec les correctifs suivants :

- Résolution d'un problème connu qui pouvait entraîner l'échec des connexions IPSEC (IP Security) ;
- Résolution d'un problème connu qui pouvait entraîner le redémarrage inattendu des serveurs Windows ;
- Résolution d'un problème qui empêche l'écriture correcte des attributs Active Directory (AD) lors d'une opération de modification LDAP (Lightweight Directory Access Protocol) lorsque vous apportez plusieurs modifications d'attribut ;
- Résolution d'un problème qui pouvait empêcher le montage d'un support amovible formaté à l'aide du système de fichiers résilient (ReFS) ou entraîner le montage du support amovible au format de fichier RAW.

Source: *https://bit.ly/3qZvwC6*

WordPress

La mise à jour de sécurité WordPress 5.8.3 corrige une injection SQL et des failles XSS

10 Janvier 2022

L'équipe de développement WordPress a publié la version 5.8.3, une version qui corrige quatre vulnérabilités, dont trois qui sont de haute gravité.
L'ensemble comprend une injection SQL sur WP_Query, une injection SQL aveugle via le WP_Meta_Query, une faille XSS via les slugs post et une injection d'objet admin.

Tous les problèmes ont des conditions préalables à leur exploitation, et la plupart des sites WordPress qui utilisent le paramètre de mises à jour automatiques par défaut ne sont pas en danger.

Les quatre failles corrigées sont :

- CVE-2022-21661 : Injection SQL de gravité élevée (score CVSS 8.0) via WP_Query.
- CVE-2022-21662 : Vulnérabilité XSS de gravité élevée (score CVSS 8.0) permettant aux auteurs (utilisateurs à privilèges inférieurs) d'ajouter une porte dérobée malveillante ou de prendre le contrôle d'un site en abusant des slugs de publication.
- CVE-2022-21663 : Problème d'injection d'objet de gravité moyenne (score CVSS 6,6) qui ne peut être exploité que si un acteur de la menace a compromis le compte administrateur.
- CVE-2022-21664 : Injection SQL de gravité élevée (score CVSS de 7,4) via la classe de base WP_Meta_Query.

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

Linux

Des vulnérabilités dans le Panneau de configuration Web exposent les serveurs Linux au piratage

22 Janvier 2022

Deux failles de sécurité critiques dans le Panneau de configuration Web exposent potentiellement les serveurs Linux à des attaques d'exécution de code à distance.

Control Web Panel est un panneau de contrôle Linux open-source populaire pour les serveurs et VPS qui permet une gestion facile des environnements d'hébergement Web.

Un attaquant pourrait enchaîner les vulnérabilités pour exécuter du code à distance sans authentification sur des serveurs Linux vulnérables.

Le premier problème, suivi sous le nom de CVE-2021-45467, est une vulnérabilité d'inclusion de fichiers qui se produit lorsqu'une application Web est amenée à exposer ou à exécuter des fichiers arbitraires sur le serveur Web.

Le deuxième problème, suivi sous le nom de CVE-2021-45466, est une vulnérabilité d'écriture de fichier arbitraire qui permet à un attaquant d'obtenir l'exécution de code à distance sur le serveur.

Les responsables de CWP ont déjà corrigé la faille avec des mises à jour de sécurité publiées ce mois-ci.

Source : *https://bit.ly/3IFbV95*

Un dangereux bug du noyau Linux a été trouvé et corrigé

21 Janvier 2022

Un nouveau problème du noyau Linux vient d'apparaître, ce dernier génère un débordement de tas dans le legacy_parse_param dans le programme fs/fs_context.c. Ce paramètre est utilisé dans les systèmes de fichiers Linux lors de la création de superblocs pour le montage et de la reconfiguration de superlocs pour un remontage. Le superbloc enregistre toutes les caractéristiques d'un système de fichiers telles que la taille du fichier, la taille du bloc, les blocs de stockage vides et remplis.

Un attaquant local peut exploiter ce bug pour augmenter ses privilèges ou bloquer le système. Cela peut être fait avec un programme spécialement conçu qui déclenche ce dépassement d'entier.

Mais avec la nouvelle mise à jour, ce problème a été résolu.

Source : *https://zd.net/3fVRD5X*

IBM

Vulnérabilité dans IBM WebSphere

25 Janvier 2022

Une nouvelle vulnérabilité trouvée dans l'application WebSphere Server Liberty d'IBM qui permet à un attaquant authentifié à distance de réaliser une injection LDAP. En utilisant une requête spécialement conçue, un attaquant pourra obtenir l'autorisation d'accéder à des ressources non autorisées. Suivie du nom CVE-2021-39031, la faille a un score de 7.5 sur l'échelle CVSS. Elle a affecté la WebSphere Application Server Liberty les versions de 17.0.0.3 à 22.0.0.1.

La solution recommandée est d'appliquer le correctif provisoire ou le Fix Pack contenant l'APAR PH42489 pour chaque version du produit nommée dès que possible. Et d'appliquer le Liberty Fix Pack 22.0.0.2 qui sera disponible dans ce premier trimestre de 2022.

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

McAfee

Correction d'une faille de sécurité qui permet d'exécuter un code arbitraire avec les privilèges systèmes dans McAfee Agent.

21 Janvier 2022

McAfee a corrigé une vulnérabilité de haute gravité, connue sous le nom de CVE-2022-0166, qui réside dans le logiciel McAfee Agent pour Windows. Un attaquant peut exploiter cette faille afin d'élever ses privilèges et d'exécuter du code arbitraire avec les privilèges du système.

La faille CVE-2022-0166 affecte les versions d'Agent antérieures à 5.7.5 et permet aux attaquants non privilégiés d'exécuter du code en utilisant les privilèges du compte NT AUTHORITY\SYSTEM.

La société de sécurité a corrigé la vulnérabilité avec la publication de McAfee Agent 5.7.5 le 18 janvier.

La vulnérabilité n'est exploitable que localement, mais les experts préviennent que ce problème pourrait être enchaîné avec d'autres problèmes pour compromettre le système cible et élever les permissions afin de mener des activités malveillantes supplémentaires.

McAfee a également corrigé une vulnérabilité d'injection de commande, repérée sous le nom de CVE-2021-31854, dans le logiciel Agent for Windows antérieur à la version 5.7.5. Un attaquant pouvait exploiter cette vulnérabilité pour injecter un code shell arbitraire dans le fichier cleanup.exe.

Source : *https://bit.ly/32yBFM9*

Actualité

Des informations d'identification volées hébergées sur VirusTotal !

Des chercheurs de SafeBreach ont découvert que VirusTotal, le célèbre service en ligne d'analyse de fichiers, d'URL et d'adresses IP suspects, peut être utilisé pour collecter des informations d'identification volées par des logiciels malveillants.

Les informations d'identification sont contenues dans des fichiers que les voleurs d'informations et les keyloggers les plus courants utilisent pour les exfiltrer des machines infectées.

Ces fichiers peuvent se retrouver hébergés sur VirusTotal parce que les pirates utilisent VirusTotal pour promouvoir la vente des données des victimes ou parce que les attaquants les téléchargent par erreur, a déclaré Tomer Bar, directeur de la recherche en sécurité chez SafeBreach. Ils peuvent également être téléchargés par des tiers qui ignorent qu'ils contiennent des informations sensibles.

Tout comme Google Search peut être utilisé pour rechercher des sites/systèmes vulnérables, les API et outils de VirusTotal (VT Graph, Retrohunt, etc.) peuvent être utilisés pour trouver des fichiers contenant des données volées.

"Un criminel qui utilise cette méthode peut recueillir un nombre presque illimité d'identifiants et d'autres données sensibles de l'utilisateur avec très peu d'efforts et en peu de temps, en utilisant une approche sans infection. Nous l'avons appelé le cybercrime parfait, non seulement en raison du fait qu'il n'y a aucun risque et que l'effort est très faible, mais aussi en raison de l'incapacité des victimes à se protéger contre ce type d'activité". Après que les victimes ont été piratées par le pirate initial, la plupart d'entre elles ont peu de visibilité sur les informations sensibles qui sont téléchargées et stockées dans VirusTotal et d'autres forums."

Les chercheurs ont exhorté Google à rechercher et à supprimer périodiquement les fichiers contenant des données sensibles sur les utilisateurs et à interdire les clés API qui téléchargent ces fichiers, ainsi qu'à ajouter un algorithme qui interdit le téléchargement de fichiers contenant des données sensibles en clair ou des fichiers cryptés avec le mot de passe de décryptage joint.

Source : https://bit.ly/3fXae1I

Une nouvelle variante du malware RedLine utilise Omicron pour piéger ses victimes

Une nouvelle variante du malware RedLine a été découverte. Elle se propage par le biais d'e-mails utilisant une fausse application de compteur de statistiques Omicron.

Cette variante a été repérée par les chercheurs de Fortinet sous la forme du fichier Omicron Stats[.]exe.

Le malware récolte les informations d'identification enregistrées sur les services VPN, notamment OpenVPN, ProtonVPN et Opera GX.

Il fouille également les dossiers Telegram pour trouver des images et des historiques de conversation et les envoie aux serveurs de l'attaquant.

En outre, il inspecte les ressources locales de Discord pour voler des journaux, des fichiers de base de données et des jetons d'accès.

En plus de la capacité de vol d'informations déjà existante, la nouvelle variante a connu de multiples améliorations telles que le vol du nom de la carte graphique, le fabricant du BIOS, le code d'identification, le numéro de série, la date de sortie, la version et les détails du fabricant du disque dur.

Il est conseillé aux équipes de sécurité de déployer une solution anti-malware fiable, de chiffrer les données importantes et d'utiliser un pare-feu réseau afin de rester protégé.

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

Les cybercriminels falsifient les codes QR pour voler les données des victimes

L'Internet Crime Complaint Center (IC3) du FBI a publié une alerte générale sur les codes QR "malveillants" qui dirigent les utilisateurs peu méfiants vers le monde de la cybercriminalité.

"Les cybercriminels tirent parti de cette technologie en dirigeant les scans de codes QR vers des sites malveillants pour voler les données des victimes, en intégrant des logiciels malveillants pour accéder à l'appareil de la victime et en redirigeant les paiements à des fins cybercriminelles", indique le communiqué.

Le communiqué du FBI ne cite aucun exemple d'une telle activité, mais précise que la supercherie se produit généralement par le biais de codes QR qui ont été modifiés, soit à l'écran, soit sur une page imprimée.

"Une victime scanne ce qu'elle pense être un code légitime, mais le code trafiqué la dirige vers un site malveillant, qui l'invite à saisir des informations de connexion et des informations financières", indique le FBI.

Il recommande aux consommateurs de vérifier toute URL générée par un code QR et d'être prudents lorsqu'ils utilisent ces codes en général, notamment pour effectuer des paiements.

Source : https://bit.ly/3fV2a1j

OceanLotus uilise le format de fichier d'archives Web pour échapper à la détection

Le groupe de pirates informatiques connu sous le nom d'OceanLotus est en train d'utiliser le format de fichier d'archive Web (.MHT et .MHTML) pour échapper à la détection des

systèmes tout en fournissant des portes dérobées pour les intrusions, selon un rapport de Netskope Threat Labs

L'attaque commence par une compression RAR d'un fichier d'archive Web de 35 à 65 Mo chargé d'un document Word malveillant. Pour contourner la protection de Microsoft Office, les attaquants définissent la propriété ZoneID des métadonnées du fichier sur 2, le faisant passer pour un fichier téléchargé depuis une source légitime.

L'ouverture du fichier d'archive web contenant le document Word infecté demande à la victime d'activer le contenu, ce qui ouvre finalement la voie à l'exécution du code de la macro VBA malveillante. Par la suite, le code macro exécute plusieurs tâches et supprime le fichier Word d'origine, conduisant au document leurre qui déclenche un faux pop-up d'erreur.

La charge utile déposée (DLL 64 bits) s'exécute toutes les 10 minutes à l'aide d'une tâche planifiée imitant la vérification de la mise à jour de WinRAR, et la porte dérobée est injectée dans le fichier rundll32[.]exe qui s'exécute indéfiniment dans la mémoire système pour éviter toute détection.

Le malware collecte différentes informations, telles que l'adaptateur réseau, une liste de répertoires et de fichiers système, le nom d'utilisateur, le nom de l'ordinateur, et vérifie la liste des processus en cours d'exécution.

Une fois les données recueillies, la porte dérobée ajoute et crypte le tout dans un seul paquet avant de l'envoyer au serveur C2 qui est hébergé sur un service de collaboration d'hébergement en nuage et de développement web, connu sous le nom de Glitch.

Source : https://bit.ly/3FWU1E7

Cloud… soyons prêts

La priorité dans la migration vers le cloud

La clé d'une migration efficace vers le cloud réside dans la planification. Pour réussir la transition, les organisations doivent commencer dès le début en créant une feuille de route pour la migration. Voici quelques éléments à prendre en compte avant d'entamer le processus :

Les dépendances entre les services : Pour déterminer comment planifier la migration, il est essentiel d'identifier les connexions entre les services et de découvrir leurs dépendances pour créer des diagrammes de dépendance clairs. En s'appuyant sur ces diagrammes, les organisations peuvent évaluer les composants à migrer et dans quel ordre. Les services ayant le moins de dépendances sont les meilleurs par lesquels commencer, les services internes migrant en premier, suivis des services les plus externes (ceux qui sont les plus proches du client).

Les applications à mission critique : De nombreuses organisations fournissent des services qui ne peuvent se permettre une réduction des performances, ou des exigences en matière de sécurité. C'est pourquoi les premiers types d'applications qu'une agence doit identifier est ceux qui sont essentiels à sa mission et qui nécessitent une posture de sécurité élevée. Ensuite, il faut commencer par les applications les moins critiques, afin de se donner le temps de comprendre le nouveau processus et de s'adapter à un faible risque avant de passer aux applications plus critiques.

Comme toujours, un bon voyage commence par une bonne planification. Les organisations doivent prendre le temps de considérer les facteurs impliqués, y compris leur allocation de risque, leur posture de sécurité actuelle, le type d'informations qu'elles vont transférer, et leur calendrier de migration. Une fois ces décisions de haut niveau prises, le reste suivra.

Sources : https://bit.ly/3AzYED3 ; https://bit.ly/32BDB6t

Bon à savoir !

Comment lutter contre le Smirshing, ou l'escroquerie par SMS ?

Suite à une augmentation alarmante des escroqueries qui usurpent des marques populaires dans des attaques de smishing (hameçonnage par SMS), le National Cyber Security Center (NCSC) du Royaume-Uni a publié de nouvelles directives pour les organisations à suivre lorsqu'elles communiquent avec leurs clients par SMS ou par téléphone.

Lorsque les organisations utilisent les SMS pour communiquer avec un public, le NCSC leur recommande d'appliquer les directives suivantes pour garantir aux destinataires qu'un texte est légitime :

- Utilisez un numéro à cinq chiffres au lieu d'un numéro de téléphone ordinaire ;
- Utilisez un SenderID qui apparaît à la place du numéro d'envoi, indiquant que l'expéditeur est digne de confiance et de l'utiliser de manière cohérente dans toutes les communications ;
- Essayez de ne pas inclure de liens web dans les SMS, mais si c'est absolument nécessaire, n'utilisez pas de services de raccourcissement d'URL qui masquent le domaine ;
- Utilisez le moins de fournisseurs de distribution de SMS possible, et vérifiez tous les messages pour en valider le contenu.

D'un autre côté, il est facile d'usurper les numéros de téléphone d'entités légitimes, de ce fait, le numéro d'appel ne donne pas une garantie de sécurité dans les communications. Pour aider à résoudre ce problème, il est conseillé aux entreprises de :

- Incitez les clients à vous appeler plutôt et fournissez des informations sur la façon de le faire sur le site officiel ;
- Assurez-vous que les fournisseurs de services n'acheminent pas les appels vers des infrastructures étrangères ;
- Assurez-vous que les fournisseurs de services respectent les "Conditions générales d'accès" ;
- Maintenez la cohérence en utilisant les mêmes numéros pour appeler les gens ;
- Fournir un moyen et des conseils aux clients pour signaler les escroqueries.

Les consommateurs doivent également faire leur part en gardant à l'esprit les points suivants :

- Les messages légitimes sont généralement cohérents et directs ;
- Le numéro de téléphone et l'adresse électronique utilisés sont minimes ;
- Les SenderIDs valides ne comportent généralement pas de caractères spéciaux ;
- La validité de l'adresse et du numéro d'envoi doit être facile à vérifier sur le site web officiel de l'entité ;
- Les communications honnêtes ne demandent jamais de détails personnels ;
- Les URL raccourcies sont un signal d'alarme ;
- En général, si quelque chose vous semble anormal lorsque vous parlez à quelqu'un, demandez-lui son nom et raccrochez. Ensuite, appelez indépendamment l'organisation en utilisant le numéro que vous trouverez sur son site web et demandez à parler à l'agent qui vous a contacté ;
- Ne donnez en aucun cas des informations personnelles sensibles lors d'appels que vous n'avez pas initiés.

Source : *https://bit.ly/3nVM7Vr*

Evènements

Evènement du mois

Les implications des médias sociaux en matière de cybersécurité

26 Décembre 2021

Online

https://bit.ly/32EjmVU

Dans cet événement, le centre de cybersécurité de l'Université du Surrey et le groupe SASIG ont abordé le sujet les implications en matière de cybersécurité dans le changement apporté par les médias sociaux, notamment :

- Que savent réellement les plateformes de médias sociaux en ligne à notre sujet ?
- Quelles sont les conséquences de l'utilisation des médias sociaux sur la vie privée et la sécurité?
- Les médias sociaux font-ils partie de l'infrastructure nationale critique ?
- Comment les cyberattaquants peuvent-ils utiliser votre présence sur les médias sociaux ?
- Quelles sont les implications en matière de sécurité de l'introduction d'un ou plusieurs métavers comme prochaine évolution des médias sociaux ?

Evènement à venir

SECURA NORTH AFRICA

22 au 24 Février 2022

SAFEX, Alger, Algérie

https://bit.ly/3AySseF

La quatrième édition du salon international de sûreté, sécurité, feu et urgences sera organisée à Alger dans les jours à venir.

L'objectif de cet événement est de rassembler au même endroit pendant 3 jours tous les acteurs et professionnels du secteur de la sécurité industrielle et commerciale, de la sécurité des travailleurs, de la lutte contre l'incendie et des urgences.

Pour cela, plusieurs acteurs du domaine seront présents comme exposant, et des conférences seront données par des experts autour des thématiques suivantes : les incendies et la gestion des crises (Jour1), la cybersécurité et le e-paiement (Jour 2 – matinée -), et la sureté, vidéo-surveillance et la vidéo-protection (Jour 2 – après-midi -).

Référence	ANPT-2022-BV-01
Titre	Bulletin de veille N°01
Date de version	31 Janvier 2022
Contact	ssi@anpt.dz