BULLETIN DE VEILLE N°03

ANPT-2022-BV-03

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

Mars 2022

Alertes de sécurité

Microsoft

71 vulnérabilités corrigées avec le Patch Tuesday

08 Mars 2022

Microsoft a publié 71 correctifs (en comptant celles de Microsoft Edge) de sécurité pour ces produits, dont 41 correctifs pour les vulnérabilités de Microsoft Windows, cinq vulnérabilités dans Microsoft Office et deux dans Microsoft Exchange.

Parmi ces vulnérabilités, deux sont considérées comme critiques « CVE-2022-22006 et CVE-2022-24501 », tandis que les autres sont considérées comme importantes.

Ces correctifs incluant des vulnérabilités d'exécution de code à distance (RCE), des bogues de déni de service, des bogues d'élévation de privilèges, des problèmes d'usurpation, des fuites d'informations et des exploits de contournement de politique, et elles ont touché les produits : Exchange, Visual Studio, l'application Xbox pour Windows, Intune, Microsoft Defender, Express Logic, Azure Site Recovery et le navigateur Microsoft Edge basé sur Chromium.

Il est fortement recommandé d'appliquer ces mises à jour afin d'éviter tout risque possible.

Source : *https://zd.net/3qE4nEf*

Android

Une critique vulnérabilité corrigée dans système Android

08 Mars 2022

Google a annoncé la publication de mise à jour de sécurité pour 39 failles pour Android qui affectent différents composants tels que Système et Cadre Média.

La vulnérabilité la plus grave est repérée sous le nom de CVE-2021-39708, un problème qui pourrait conduire à une élévation de privilèges exploitable à distance identifié dans le composant Système.

Au total, 10 failles de sécurité ont été résolues dans le composant System (neuf élévations de privilèges et une vulnérabilité de divulgation d'informations), six ont été résolues dans Framework (quatre élévations de privilèges et deux dénis de service), une a été corrigée dans Android runtime (élévation de privilèges) et une dans Media Framework (divulgation d'informations).

Les correctifs résolvent également 21 vulnérabilités dans le composant 'Cadre', elles ont un impact sur les composants Framework, Kernel, MediaTek, Qualcomm et Qualcomm closed-source.

Les utilisateurs d'Android sont invités à appliquer les mises à jour disponibles sur le site officiel d'Android.

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

Sophos

Un bogue RCE dans les pares-feux Sophos

27 Mars 2022

Sophos a corrigé une vulnérabilité critique qui réside dans les zones 'User Portal' et 'Webadmin' de Sophos Firewall, et elle permet l'exécution de code à distance (RCE).

La faille connue sous le nom de CVE-2022-1040 a reçu un score CVSS de 9.8 et affecte les versions 18.5 MR3 (18.5.3) et antérieures de Sophos Firewall.

Un attaquant distant disposant d'un accès au portail utilisateur ou à l'interface Webadmin du pare-feu peut exploiter cette faille pour contourner l'authentification et exécuter du code arbitraire.

D'après l'entreprise, les clients sont recommandés à ne pas exposer leur portail utilisateur et leur Webadmin au WAN, même après l'application du correctif.

Source : *https://bit.ly/3iIl0dm*

HP

Plusieurs modèles d'imprimantes HP sont vulnérables à l'exécution de code à distance

22 Mars 2022

Quatre vulnérabilités ont été corrigé dans certains modèles d'imprimantes HP 'LaserJet Pro', 'Pagewide Pro', 'OfficeJet', 'Enterprise', 'Large Format' et 'DeskJet'.

La première suivie sous le nom de CVE-2022-3942 avec un score de 8.4 sur l'échelle CVSS, est une faille de débordement de tampon qui pourrait permettre à un acteur de menace d'exécuter de code à distance sur la machine affectée.

Les trois restantes pourraient être exploitées pour la divulgation d'informations, l'exécution de code à distance et le déni de service, répertoriées sous les noms de CVE-2022-24291 (score CVSS : 7.5), CVE-2022-24292 (score CVSS : 9.8) et CVE-2022-24293 (score CVSS :9.8).
Il est recommandé d'appliquer les mises à jour de sécurité dès que possible, de placer les appareils derrière un pare-feu réseau et de mettre en place des politiques de limitation de l'accès à distance.

Source : *https://bit.ly/3Nuw8ZJ*

Microweber

Microweber corrige une vulnérabilité XSS dans le système de gestion de contenu 'CMS'

24 Mars 2022

Une vulnérabilité de type 'cross-site scripting' (XSS) a été découverte dans Microweber, un créateur de sites web et système de gestion de contenu (CMS) open source.

Suivie sous le nom de CVE-2022-0930, cette faille est due à des lacunes dans protections de filtrage de contenu offertes par les versions antérieures à 1.2.12 de Microweber.

Ces lacunes permettaient aux attaquants de télécharger une charge utile XSS, à condition qu'elle contienne un fichier dont le nom se termine par "html"

Une fois cette charge utile téléchargée, il est possible d'accéder à une URL contenant du HTML malveillant et d'exécuter du JavaScript malveillant. Ensuite, il sera possible pour l'attaquant de voler des cookies avant de se faire passer pour la victime, éventuellement l'administrateur d'un système compromis.

Microweber confirme que le problème est résolu et invite ses clients à passer vers la version corrigée afin d'atténuer toute menace possible.

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

SonicWall

Vulnérabilité dans les produits SonicWall

25 Mars 2022

Une faille de gravité critique a été corrigé dans les pares-feux de SonicWall qui peut permettre à un acteur de menace distant non authentifié causer un déni de service (DoS) ou d'entraîner éventuellement l'exécution de code dans le système vulnérable.

Répertoriée sous le nom de CVE-2022-22274 avec une évaluation de 9.4 sur le système d'évaluation des vulnérabilités CVSS. Ce bogue est dû à un débordement de tampon basé sur la pile dans le SonicOS via une requête http.

En attendant que les correctifs puissent être appliqués, SonicWall recommande fortement les administrateurs de limiter l'accès à la gestion de SonicOS aux sources fiables en modifiant les règles d'accès à la gestion de SonicOS (SSH/HTTPS/HTTP Management). Cette modification permettra uniquement l'accès à la gestion à partir d'adresses IP de sources fiables.

Les administrateurs sont invités aussi à appliquer les correctifs pour les versions corrigées pour éviter l'exploitation de cette faille.

Source : *https://bit.ly/3iF9hwj*

Honda

Le bogue de Honda permet le déverrouillage et le démarrage à distance d'une voiture

25 Mars 2022

Des chercheurs ont découvert une vulnérabilité de type "replay attack" affectant certains modèles de voitures Honda et Acura fabriquée entre 2016 et 2020, qui peut permettre à un attaquant situé à faible distance de déverrouiller la voiture et même démarrer son moteur.

Cette faille de sécurité, marquée CVE-2022-27254, elle est réalisée en capturant les signaux RF envoyés par la télécommande à la voiture et les renvoie pour prendre le contrôle du système de télé-déverrouillage.

Selon les chercheurs, divers véhicules Honda envoient le même signal RF non crypté pour chaque ouverture de porte, fermeture de porte, ouverture de démarrage et démarrage à distance. Cela permet à un attaquant d'écouter la demande et de mener une attaque par relecture.

D'après BleepingComputer, Honda n'a pas l'intention de mettre à jour les véhicules plus anciens pour le moment, ce qui signifie que les consommateurs doivent prendre leurs mesures de sécurité pour remédier à ce problème.

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

Red Hat

Plusieurs vulnérabilités dans le noyau Linux de Red Hat

29 Mars 2022

Une nouvelle mise à jour a été publiée pour corriger plusieurs vulnérabilités affectant Red Hat Enterprise Linux Server, elles pourraient permettre à utilisateur malveillant de provoquer un déni de service (DoS) et une élévation de privilèges.

Cette mise à jour contient des correctifs pour cinq vulnérabilités à impact important et qui portent les noms :

- CVE-2020-0466 et CVE-2021-0920 : Des vulnérabilités qui peuvent conduire à une escalade de privilèges.
- CVE-2021-4083 : Une faille de mémoire en lecture après libération permet à un utilisateur local de planter le système ou d'escalader ses privilèges sur le système affecté.
- CVE-2022-0330 : Une faille d'accès à la mémoire aléatoire qui permet une escalade des privilèges.
- CVE-2022-22942 : Un échec de la copie d'utilisation permet l'exploitation de type use-after-free.

Les clients de Red Hat sont recommandés à mettre à jour leurs systèmes afin d'atténuer tout risque possible.

Source : *https://bit.ly/3tMuoD7*

Actualité

Microsoft confirme avoir été piraté par le groupe Lapsus$.

Microsoft a confirmé que l'un de ses employés a été compromis par le groupe de pirates Lapsus$, ce qui a permis aux acteurs de la menace de voler des parties de son code source.

Le groupe Lapsus$ a publié 37 Go de code source volé sur le serveur Azure DevOps de Microsoft. Le code source concerne divers projets internes de Microsoft, notamment pour Bing, Cortana et Bing Maps.

Dans un nouveau billet de blog publié, Microsoft a confirmé que le compte d'un de ses employés a été compromis par Lapsus$, offrant un accès limité aux dépôts de code source.

Il est fortement conseillé aux administrateurs de sécurité et de réseau de se familiariser avec les tactiques utilisées par ce groupe en lisant le rapport de Microsoft.

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

Samsung et NVIDIA, victimes du même groupe

Lapsus$ a affirmé avoir volé 190 Go de données confidentielles, y compris le code source, sur les serveurs du géant Samsung. Le groupe a également mis en ligne des clichés de ces données.

Samsung a confirmé, sans nommer le groupe de pirates, qu'il y a eu une violation de sécurité, mais elle a affirmé qu'aucune information personnelle des clients n'a été compromise.

"Nous avons récemment été informés de l'existence d'une violation de sécurité concernant certaines données internes de l'entreprise. Immédiatement après avoir découvert l'incident, nous avons renforcé notre système de sécurité", a déclaré l'entreprise.

"Selon notre analyse initiale, la violation concerne certains codes sources relatifs au fonctionnement des appareils Galaxy, mais n'inclut pas les informations personnelles de nos consommateurs ou employés. Actuellement, nous ne prévoyons pas d'impact sur nos activités ou nos clients. Nous avons mis en place des mesures pour prévenir d'autres incidents de ce type et nous continuerons à servir nos clients sans interruption."

De son coté, NVIDIA a également affirmé avoir subi une cyberattaque au cours de laquelle le même groupe a volé les informations d'identification et des données de la société.

La fuite comprenait deux certificats de signature de code volés utilisés pour signer les pilotes et les exécutables par les développeurs de NVIDIA.

Après que le groupe a divulgué les certificats de signature de code de NVIDIA, ces derniers ont été utilisés par divers acteurs de menace pour signer des logiciels malveillants.

Les deux certificats NVIDIA volés ont expiré. Cependant, Windows autorise toujours le chargement d'un pilote signé avec ces certificats. Ainsi, les programmes malveillants ressemblent à des programmes NVIDIA légitimes.

L'utilisation récente d'un certificat NVIDIA volé est un parfait exemple de l'empressement des cybercriminels à abuser de tout ce qui peut faire défaut dans l'infrastructure de sécurité. Pour éviter cette menace, il est conseillé aux administrateurs de configurer les politiques de contrôle des applications de Windows Defender pour contrôler les pilotes NVIDIA chargés dans le système d'exploitation Windows.

***Sources** : https://zd.net/3NsqzLe ; https://bit.ly/387SL5W*

Des centaines de sites hébergés par GoDaddy ont été infectés

Des analystes de sécurité de Wordfence ont constaté un pic d'infections par porte dérobée sur des sites Web WordPress hébergés par le service Managed WordPress de GoDaddy, toutes comportant une charge utile identique.

L'affaire touche des revendeurs de services Internet tels que MediaTemple, tsoHost, 123Reg, Domain Factory, Heart Internet et Host Europe Managed WordPress.

La campagne utilise principalement des modèles de spam pharmaceutiques, servis aux visiteurs des sites Web compromis à la place du contenu réel.

L'objectif de ces modèles est d'inciter les victimes à acheter de faux produits, ce qui entraîne la perte d'argent et de données de paiement pour les acteurs de la menace.

En outre, les acteurs peuvent nuire à la réputation d'un site Web en modifiant son contenu et en rendant la violation évidente.

Ce type d'attaque est plus difficile à détecter et à arrêter du côté de l'utilisateur, car elle a lieu sur le serveur et non sur le navigateur, et les outils de sécurité Internet locaux ne détecteront donc rien de suspect.

Le vecteur d'intrusion n'a pas été déterminé, donc bien que cela ressemble étrangement à une attaque de la chaîne d'approvisionnement, cela n'a pas été confirmé.

Si votre site Web est hébergé sur la plateforme Managed WordPress de GoDaddy, assurez-vous d'analyser votre fichier wp-config.php pour localiser les injections potentielles de porte dérobée.

Wordfence rappelle également aux administrateurs que si la suppression de la porte dérobée doit être la première étape, la suppression des résultats de moteurs de recherche indésirables doit également être une priorité.

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

Interruption des services GitHub

GitHub indique qu'il y a eu quatre interruptions de service le 16 mars, le 17 mars, le 22 mars et le 23 mars, et explique que ces pannes ont été causées par des problèmes de "contention des

ressources" dans leur cluster MySQL primaire appelé "MySQL1".

"Le thème sous-jacent de nos problèmes au cours des dernières semaines est dû à la contention des ressources dans notre cluster mysql1, ce qui a eu un impact sur les performances d'un grand nombre de nos services et fonctionnalités pendant les périodes de charge maximale", explique un post GitHub sur les pannes.

On parle de contention des ressources lorsque plusieurs processus demandent les mêmes ressources, qu'il s'agisse de l'utilisation de la mémoire, du processeur ou du disque, ou même de l'accès à une table de base de données.

Lorsqu'il n'y a pas assez de ressources disponibles, une base de données ne peut pas terminer les requêtes aussi rapidement, ce qui entraîne le verrouillage des tables et l'accumulation rapide des connexions à la base de données pendant qu'elles attendent la fin des requêtes.

Au fur et à mesure que les demandes s'accumulent, le serveur finit par atteindre le nombre maximal de connexions qu'il est configuré pour gérer, et rejette simplement toutes les autres demandes jusqu'à ce qu'il y ait de la place pour d'autres.

Afin d'éviter ce type de pannes à l'avenir, GitHub déclare qu'il procède à un audit de ses systèmes pendant les heures de pointe et qu'il mettra en place des correctifs de performance en fonction des résultats.

Ils redirigent également le trafic vers d'autres bases de données afin de réduire la charge et augmentent l'infrastructure et le sharding pour améliorer les performances.

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

La nouvelle menace de backdoor Linux B1txor20 utilise le tunneling DNS

Un botnet récemment découvert, cible les systèmes Linux et tente de les faire entrer dans une armée de bots prêts à voler des informations sensibles, à installer des rootkits, à créer des reverse shells et à agir comme des proxys de trafic web.

Le nouveau malware, baptisé B1txor20 par les chercheurs du laboratoire de recherche sur la sécurité des réseaux de Qihoo 360 (360 Netlab), concentre ses attaques sur les dispositifs Linux ARM et à architecture de processeur X64.

Le botnet utilise des exploits ciblant la vulnérabilité Log4J pour infecter de nouveaux hôtes, un vecteur d'attaque très intéressant étant donné que des dizaines de fournisseurs utilisent la bibliothèque de journalisation vulnérable Apache Log4j.

Au total, ils ont capturé quatre échantillons de malwares, avec des fonctionnalités de backdoor, de proxy SOCKS5, de téléchargement de malwares, de vol de données, d'exécution de commandes arbitraires et d'installation de rootkit.

Cependant, ce qui distingue le malware B1txor20, c'est l'utilisation du tunneling DNS pour les canaux de communication avec le serveur de commande et de contrôle (C2), une technique ancienne mais toujours fiable utilisée par les acteurs de la menace pour exploiter le protocole DNS afin de tunneliser les malwares et les données via des requêtes DNS.

Les chercheurs de 360 Netlab ont également constaté que si les développeurs du malware ont inclus un ensemble plus large de fonctionnalités, toutes ne sont pas activées.

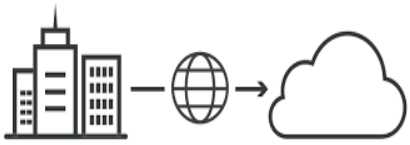
C'est probablement un signe que les fonctionnalités désactivées sont encore boguées, et que les créateurs de B1txor20 travaillent encore à les améliorer et à les activer à l'avenir.

Des informations supplémentaires, notamment les indicateurs de compromission (IOC) et une liste de toutes les instructions C2 prises en charge, sont disponibles à la fin du rapport de 360 Netlab.

Source : *https://bit.ly/3iET9ef*

Cloud… soyons prêts

L'exécution de la migration vers le cloud



Une fois que l'environnement a été évalué et qu'un plan a été élaboré, il est nécessaire d'exécuter la migration.

Le principal défi consiste à effectuer la migration en perturbant le moins possible le fonctionnement normal de l'entreprise. Ceci nécessite une visibilité durant chaque étape de la migration afin de pouvoir détecter et gérer les moindres problèmes dès qu'ils apparaissent.

Il est conseillé de commencer la transition avec des diagrammes à jour et des plans visuels de projet de migration vers le cloud accessibles à toutes les personnes concernées.

La visualisation de la migration à chaque étape de la transition permet d'appuyer sur une source unique de vérité lorsque des questions se posent, garantissant ainsi que chacun dispose du contexte dont il a besoin pour construire une infrastructure sûre, conforme et stable.

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

Bon à savoir !

Qu'est-ce qui rend les mots de passe vulnérables ?

Les attaques contre les mots de passe sont en augmentation car les mots de passe eux-mêmes sont très vulnérables aux attaques. Le rapport de Specops Software sur les mots de passe faibles de cette année a confirmé que les mots de passe sont le maillon faible du réseau d'une entreprise.

Parmi les principaux résultats obtenus dans ce rapport :

- 93% des mots de passe utilisés dans les attaques par brute force comprennent 8 caractères ou plus.
- 54 % des entreprises ne disposent pas d'un outil de gestion des mots de passe professionnel.
- 68 % des mots de passe utilisés lors d'attaques réelles comprennent au moins deux types de caractères.

Pour réduire la probabilité que les mots de passe seront compromis, il est nécessaire de se défendre contre ses attaques en appliquant les bonnes pratiques suivantes :

1. Eviter les mots de passe de 8-12 caractères (ou alors moins) car la majorité des dictionnaires utilisés dans les attaques brute force contient des mots de passe de cette longueur. Cela signifie que plus le mot de passe est long, plus il est fort.
2. Ne pas utiliser des références dans les mots de passe tels que les dates de naissance, les noms, les films préférés, etc.
3. Utiliser un mot de passe complexe en combinant des lettres majuscules et minuscules, des chiffres et plus de 2 symboles.
4. Ne jamais réutiliser le même mot de passe pour plusieurs comptes, il faut créer un mot de passe pour chaque compte. Pour éviter le fait d'oublier ces mots de passe, utiliser un gestionnaire de mot de passe professionnel.
5. Changer périodiquement les mots de passe.

PS : pour une meilleure protection contre les attaques de mots de passes, il est recommandé de combiner tous les conseils ci-dessus.

Source : *https://bit.ly/3Lryt5A*

Evènements

Evènement du mois

Rétablir la confiance et l'intégrité dans la cybersécurité

30 Mars 2022

Online

https://bit.ly/3qLEYbA

Dans ce webcast, un panel de leaders de professionnels réunis par The Knowledge Group fournira et présentera une analyse approfondie des principes fondamentaux ainsi que des développements récents en matière de restauration de la confiance et de l'intégrité dans la cybersécurité. Les intervenants présenteront également toutes les questions importantes entourant ce sujet majeur. Les principaux sujets abordés sont les suivants :

- Vue d'ensemble du décret sur l'amélioration de la cybersécurité de la nation ;
- Tendances et développements en matière de cybersécurité
- Types courants de vulnérabilités en matière de cybersécurité en 2021 ;
- Stratégies pour protéger les fichiers contre les menaces les plus avancées ;
- Prévisions en matière de cybersécurité pour 2021.

Evènement à venir

Introduction à la cybersécurité

17 Avril 2022

Online

https://bit.ly/3NwqpT2

Ce webinaire sera présenté afin de permettre à l'audience de découvrir le monde de la cybersécurité et la protection des données numériques.

Les sujets qui seront abordés sont les suivants :

- Qu'est-ce que la cybersécurité ?
- Quels sont les problèmes de sécurité dans le domaine de la cybersécurité ?
- Comment maintenir la sécurité du champ cybernétique qui nous entoure ?
- Certification en cybersécurité.

Référence	ANPT-2022-BV-03
Titre	Bulletin de veille N°03
Date de version	31 Mars 2022
Contact	ssi@anpt.dz