BULLETIN DE VEILLE N°06

ANPT-2021-BV-06

« It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it. » -Stephane Nappo-

juin 2021

Alertes de sécurité

VMWARE

Vulnérabilités dans Vmware Carbon Black et Vmware tools

24 Juin 2021

Deux vulnérabilités très critiques ont été corrigées par Vmware.

La première, référencée CVE-2021-21998, est un contournement d'authentification qui affecte plusieurs versions de Vmware Carbon Black App control (AppC), ce qui peut mener à l'obtention de privilèges administrateur.

La seconde vulnérabilité, étiquetée CVE-2021-21998, affecterait Vmware Tools pour Windows. Vmware remonte Console pour Windows (VMRC pour Windows) et Vmware App Volumes. Cette vulnérabilité permettrait d'exécuter du code avec des privilèges élevés.

Il est fortement recommandé aux administrateurs systèmes et aux utilisateurs de ces produits d'installer les dernières mises à jour publiées par Vmware.

Source : *https://bit.ly/3A2AQae*

Microsoft

Patch Tuesday Microsft

08 Juin 2021

Microsoft a publié le Patch Tuesday de Juin 2021, comprenant un total de 50 vulnérabilités corrigées, dont 5 considérées comme critiques et 7 failles Zéro Day qui peuvent conduire à une élévation de privilèges ou l'exécution de code à distance.
Ces corrections ont touché de nombreux produits, notamment .NET Core, Visual Studio et VSCode, la suite Microsoft Office, Microsoft Edge, SharePoint Server, Hyper-V, Windows HTML Platform, et Windows Remote Desktop.
Les entreprises sont invitées à consulter le résumé et les informations de déploiement de la mise à jour de sécurité de juin 2021 de Microsoft et à les appliquer.

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

Cisco

De nombreuses vulnérabilités de haute gravité dans les produits Cisco

17 Juin 2021

De multiples vulnérabilités ont été découvertes et corrigées dans les produits Cisco. La vulnérabilité la plus grave de cette série de correctifs est répertoriée sous le nom de CVE-2021-1542, dans les commutateurs intelligents de la série Cisco Small Business 220. Un attaquant pourrait l'utiliser pour contourner les protections d'authentification et obtenir des privilèges administratifs sur le commutateur.
Les autres bugs de haute gravité que Cisco a corrigés comprennent la vulnérabilité de validation de certificat (CVE-2021-1566) dans Cisco Email Security Appliance et Cisco Web Security Appliance et la vulnérabilité (CVE-2021-1134) dans le Cisco DNA Center. Leur exploitation pourrait permettre à un attaquant distant non authentifié d'obtenir un accès non autorisé à des données sensibles.
Cisco a également publié des correctifs pour des problèmes de gravité moyenne dans AnyConnect, Jabber, Meeting Server, Unified Intelligence Center et Webex.
Il est recommandé aux administrateurs réseau d'appliquer les correctifs sur l'ensemble des équipements Cisco affectées.

Source : *https://bit.ly/3quTvr1*

Chrome

Google publie des correctifs pour des vulnérabilités Zero-day dans Chrome

10/17 Juin 2021

Google a corrigé plusieurs vulnérabilités dans Chrome ce mois-ci dont deux Zero-days. Les deux classées comme étant critiques et avec des exploits actifs dans la nature.
La première est référencée CVE-2021-30551, elle réside dans le moteur JavaScript V8. Elle permet à un attaquant distant

d'exploiter potentiellement une corruption de mémoire induisant à l'exécution de code arbitraire.
Et la seconde, référencée est CVE-2021-30554, est localisée dans Web Graphics Library. Elle pourrait entraîner un crash, ou même l'exécution de code ou de commandes non autorisés.
Il est recommandé aux utilisateurs de Google Chrome d'effectuer une mise à jour vers la dernière version (91.0.4472.114).

Source : https://bit.ly/3gYS68F
https://bit.ly/3hgxbNm

Linux

Une vulnérabilité Linux qui date de 7ans

11 Juin 2021

Une vulnérabilité d'élévation de privilèges vieille de sept ans se cachait dans plusieurs distributions Linux. Cette dernière a été corrigée le 03 juin 2021. Cette vulnérabilité dans le service système *Polkit* (Policy kit) pourrait être exploitée par un attaquant local malveillant non privilégié pour contourner l'autorisation et élever les autorisations à l'utilisateur root.

Référencée par CVE-2021-3560 (score CVSS : 7,8), la faille affecte les versions de *Polkit* entre 0,113 et 0,118 dans les distributions linux comme Debian (unstable), RHEL 8, Fedora 21+ et Ubuntu 20.04.

Il est donc important de mettre à jour les installations Linux dès que possible.

Source : https://bit.ly/3h4usbf

Une vulnérabilité non corrigée dans Pling store de linux

22 Juin 2021

Des spécialistes de la cybersécurité à l'agence Positive Security ont signalé une vulnérabilité critique non corrigée qui touche Plingstore de Linux. Cette vulnérabilité pourrait être exploitée pour organiser des attaques de type « supply chaine » et permettre l'exécution de code à distance (RCE).
Une autre faille XSS a été découverte dans les extensions de GNOME Shell et des extensions qui contient de porte dérobée ont même été publiées.
Étant donné que la faille RCE associée à PlingStore n'a pas encore été résolue, il est recommandé de ne pas exécuter l'application Electron jusqu'à ce qu'un correctif soit publié.

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

Adobe

41 vulnérabilités corrigées par adobe

08 Juin 2021

Adobe a publié 10 mises à jour de sécurité concernant 41 CVE de plusieurs produits, ayant différents niveaux de criticité. Certaines de ces vulnérabilités peuvent causer une élévation de privilèges comme le CVE-2021-28623 et le CVE-2021-28597 qui ont touché Adobe Premiere et Photoshop respectivement. D'autres vulnérabilités peuvent amener à l'exécution de code arbitraire (CVE-2021-28588 et CVE-2021-28622) sur Adobe Animate et RoboHelp Server respectivement.

Aussi, des vulnérabilités moins critiques peuvent conduire également à une divulgation d'information ou un déni de service.
Aucune des vulnérabilités corrigées dans ce lot de mises à jour de sécurité ne fait l'objet d'attaques actives.

Source: https://bit.ly/3h011qy

Wordpress

Une vulnérabilité dans un plugin Wordpress permet le téléchargement des logiciels malveillants sur les sites

02 Juin 2021

Il a été découvert que Fancy Product Designer, un plugin WordPress installé sur plus de 17 000 sites, contient une vulnérabilité critique qui est activement exploitée pour télécharger des logiciels malveillants sur les sites sur lesquels le plugin est installé. Ainsi, un attaquant pourrait exécuter un code à distance, ce qui permettrait une prise de contrôle totale du site.

Une version corrigée de Fancy Product Designer (4.6.9) a été publiée. Il est donc conseillé aux administrateurs des sites Web utilisant le plugin de le corriger immédiatement.

Source : https://bit.ly/3x3Ulxo

Apple

Apple corrige un bug dans macOS qui pourrait causer des élévations de privilèges

03 Juin 2021

Trend Micro, un fournisseur de solutions de cybersécurité, a découvert une vulnérabilité dans macOS enracinée dans le Core Virtual Machine Server (CVMServer). La vulnérabilité, étiquetée CVE-2021-30724, peut conduire à une élévation de privilèges. Elle affecte les appareils exécutant des versions anciennes de macOS Big Sur 11.4, iOS 14.6 et iPadOS 14.6.

Les utilisateurs doivent maintenir leurs appareils à jour pour recevoir les derniers correctifs. Apple a publié les mises à jour de sécurité qui traitent ce problème, à savoir macOS Big Sur 11.4, iOS 14.6 et iPadOS 14.6.

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

Western Digital

Une Vulnérabilité non corrigée dans My Book Live

24 Juin 2021

Le 24 juin 2021, des utilisateurs de *My Book Live* n'ont pas pu accéder à leurs données. Les journaux ont révélé que les appareils avaient reçu une commande à distance pour une réinitialisation d'usine.

La dernière mise à jour publiée par WD remonte à 2015 malgré la découverte de la vulnérabilité référencée CVE-2018-18472 qui a une criticité de 9,8 permettant à toute personne ayant l'adresse IP du NAS d'exécuter des commandes sur l'appareil en tant que root. Aucune correction n'a été publiée, faisant d'elle la cause la plus évidente de l'incident.

Pour tout utilisateur de NAS qui n'a pas encore perdu ses données, déconnectez-le immédiatement.

Source : https://bit.ly/3y4nJ6K

Actualité

Une nouvelle politique de sécurité pour github

05 Juin 2021

GitHub a officiellement annoncé le 04 Juin une série de mises à jour des politiques du site qui approfondissent la façon dont la société traite les logiciels malveillants et les codes d'exploitation téléchargés sur son service.

Déclarant qu'elle n'autorisera pas l'utilisation de GitHub pour soutenir directement des attaques illégales ou des campagnes de logiciels malveillants, la société a indiqué qu'elle pourrait prendre des mesures pour perturber les attaques en cours qui utilisent la plateforme comme un réseau de diffusion de contenu de logiciels malveillants.

Dans les scénarios où il y a un abus actif et généralisé de contenu à double usage, la société a déclaré qu'elle pourrait restreindre l'accès à ce contenu en le plaçant derrière des barrières d'authentification et, en "dernier recours", désactiver l'accès ou supprimer le code complètement lorsqu'il est incorporé directement dans une campagne malveillantes active.

Source : *https://bit.ly/3deX4Mo*

ALPACA la nouvelle technique d'attaque TLS

09 Juin 2021

Des chercheurs ont divulgué un nouveau type d'attaque nommé ALPACA (Application Layer Protocol Confusion - Analyzing and mitigating Cracks in TLS Authentication), qui exploite les mauvaises configurations des serveurs de sécurité de la couche de transport (TLS) pour rediriger le trafic HTTPS du navigateur Web d'une victime vers un autre point de terminaison de service TLS situé sur une autre adresse IP afin de voler des informations sensibles.

Les attaques ALPACA sont possibles car TLS ne lie pas la connexion TCP au protocole de l'application. Dans le cas où différents services utilisent des certificats compatibles, il est possible de rediriger leur trafic de l'un à l'autre sans que le navigateur de la victime ne reçoive d'avertissement de sécurité.

En d'autres termes, la technique utilisée consiste en une attaque Man-in-the-Middle dans laquelle un attaquant intercepte et redirige la connexion HTTPS d'une victime vers un autre service protégé par TLS et des certificats compatibles. Par conséquent, elle peut être exploitée pour exfiltrer des cookies de session ou d'autres données privées ou même exécuter des attaques Cross Site Scripting (XSS).

Pour empêcher les attaques inter-protocoles, les chercheurs proposent d'utiliser les extensions ALPN (Application Layer Protocol Negotiation) et SNI (Server Name Indication) de TLS, qui peuvent être utilisées par un client pour indiquer au serveur, au début du processus d'établissement de la connexion, le protocole qu'il souhaite utiliser sur une connexion sécurisée et le nom d'hôte auquel il tente de se connecter.

Source : *https://bit.ly/3diRJ6C*

Attaques massives ciblant les VPN

17 Juin 2021

L'utilisation du VPN a remarquablement augmenté au cours du premier trimestre 2021 due à la pandémie du Covid19 et les changements qu'elle a engendrés allant du télétravail, jusqu'à l'accès aux ressources des universités à distance.

En plus de leur exploitation habituelle par les utilisateurs en naviguant sur internet. Cette popularité d'usage des VPN les a transformés en une cible plus commune pour les cyberattaques.

Rien que depuis le début de l'année 2021, d'après le rapport de Nuspire -fournisseur de services de sécurité- les attaques contre le VPN SSL de Fortinet ont augmenté de 1.916%, et celles contre le VPN sécurisé de Pulse Connect de 1.527%. Ce mois-ci, de nombreuses attaques de VPN ont été commises comme celle de Colonial Pipeline conduisant à la perturbation de l'approvisionnement en carburant dans plusieurs Etats Américains à cause d'un mot de passe de VPN compromis.

Un autre exemple est l'attaque qui a visé le VPN publique Psiphon pour désamorcer un trojan dans les machines des utilisateurs pour collecter leurs informations personnelles depuis au moins 2015.

Il est donc indispensable pour les organisations de suivre les bonnes pratiques et de maintenir à jour les technologies VPN utilisées.

Source : *https://bit.ly/3dj7hr3*

Le monde du jeu en danger !

10 Juin 2021

L'industrie des jeux en ligne a connu une forte progression, en grande partie due à la pandémie, beaucoup se tournant vers les jeux en ligne pour échapper à la routine quotidienne stressante.

Cependant, en raison de sa dépendance à la connectivité, l'industrie et la communauté des joueurs ne sont pas à l'abri des menaces de cybersécurité. Des informations sensibles, tant personnelles que financières, sont utilisées, stockées et liées aux comptes de jeux en ligne.

Dans ces derniers mois seulement, plusieurs entreprises de jeux vidéo ont été ciblées par des cyber-attaques comme En

novembre, des pirates informatiques ont infiltré le réseau informatique de l'éditeur japonais Capcom (Street Fighter, Resident Evil). Un mois plus tôt, la société française Ubisoft et la société allemande Crytek ont été victimes d'un Ransomeware de la part du groupe de hackers Egregor. En février, le studio CD Projekt Red (Cyberpunk 2077, The Witcher) a également été attaqué d'un ransomeware par des pirates informatiques affirmant avoir récupéré du code source.

Et l'attaque la plus récente et qui a marqué l'industrie du jeux vidéo est celle ciblant l'éditeur américain EA (electronic arts : développeur et producteur de jeux vidéo) qui a été victime d'un vol de données le 10 juin 2021. Des attaquants ont réussi à pénétrer son système d'information et à dérober 780 Go de données, dont le code source de son célèbre jeu de football Fifa 2021-2022.

Selon un rapport d'Akamai Technologies, entre juillet 2019 et juin 2020, l'industrie du jeu a été également victime de 3 000 des 5 600 attaques par déni de service (qui visent à saturer les serveurs pour les rendre indisponibles), ce qui en fait de loin le secteur le plus visé.

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

Cloud… soyons prêts !

Quelle activité ? quelle donnée à mettre sur le Cloud ?

En voulant intégrer le Cloud au sein d'une entreprise, une des premières questions à se poser est : Faut-il tout mettre dans le Cloud? Sinon, quelles activités et quelles données mettre dans le cloud ?

En effet, la réponse à ces questions se trouve dans le principal objectif de l'entreprise quand elle a fait recours au cloud. Les activités que l'entreprise décide d'introduire dans le Cloud doivent s'en retrouver bonifier d'un gain significatif, qui peut être la réduction des couts, la flexibilité, l'accès aux ressources de l'entreprise de manière simplifiée, etc.

Ce gain n'est pas le seul indicateur qui doit influencer cette décision, d'autres aspects sont aussi à prendre en considération, tels que :

- La sécurité : Une classification des données selon leurs criticités doit être faite, afin de décider lesquelles conserver en internes et celles à mettre sur le Cloud ;
- L'aspect économique : Une évaluation et comparaison doit être faite pour choisir les activités qui vont être mises sur le cloud afin de mieux tirer parti de ce service et maximiser les bénéficies de l'entreprise ;
- Les limites législatives ou normatives : L'entreprise doit être au courent de toutes les lois à prendre en compte dans cette prise de décision ainsi que les normes auxquelles elle doit être conforme.

Source : *https://bit.ly/35RinQ*

Bon à savoir !

Gestion des mots de passes : Risques et bonnes pratiques

Yubico, une entreprise de cybersécurité, a publié les résultats d'une étude sur l'adaptabilité des entreprises au télétravail et les attitudes actuelles des employés vis-à-vis de la cybersecurité. Le rapport a interrogé plus que 3 000 employés.

Les statistiques ont révélé que 54 % des employés utilisent les mêmes mots de passe sur plusieurs comptes professionnels. 22 % des personnes interrogées gardent encore la trace des mots de passe en les écrivant, dont 41 % sont des chefs d'entreprise et 32 % des cadres supérieurs. 42 % des personnes interrogées admettent utiliser quotidiennement des appareils fournis par leur employeur à des fins personnelles.

Les personnes qui utilisent le même mot de passe contribuent involontairement à l'augmentation des fraudes de compte. Si un pirate obtient l'accès à un compte utilisateur, il peut facilement prendre le contrôle de tous les comptes en ligne et d'accéder aux données professionnelles et personnelles.

En conséquent, est fortement recommandé de :

- Utiliser un mot de passe différent pour chaque plateforme ;
- Utiliser des mots de passes forts d'au moins 10 caractères incluant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux, de telle sorte qu'ils ne peuvent pas être prédits facilement ;
- Utiliser l'authentification à deux facteurs, quand c'est possible ;

- Ne pas écrire les mots de passes sur des papiers et ne les communiquer à personne ;
- Changer les mots de passes périodiquement ;

Nb : Les employés de l'ANPT sont invités a consulté la campagne de sensibilisation faite sur la sécurité des mots de passe ici, ainsi que celle relative à la sécurité de la messagerie électronique ici.

Source : *https://bit.ly/3dkCjf29*
https://bit.ly/3dmsPmS
https://bit.ly/3ha2zxe

Evènements

Evènements du mois

30 Juin 2021, 4:00 - 5:00 PM

Online

https://bit.ly/361BqXO

Les attaques ransomwares ont connu une croissance alarmante ces dernières années, ce qui a rendu la lutte contre eux un défi sans précédent pour les entreprises.

Dans ce contexte, cet évènement a été animé par Adam Swan, un ingénieur senior en Threat Hunting chez SOC Prime, afin de partager ses connaissances sur les dernières évolutions des ransomwares, les techniques et les procédures appliquées par les groupes de hacker les plus prolifiques ainsi que les pratiques essentiels à appliquer pour éviter de perturber les opérations des entreprises.

Evènements à venir

Samedi 3 Juillet 2021

IGEE ex INELEC – Boumerdes

https:/ /bit.ly/35UiESf

Organisé par le club Shellmates, l'évènement HackINI, le point de rencontre des passionnées de la cybersécurité revient cette année dans sa 9ème édition.

Cet évènement vise à initier les participants au monde de la cybersécurité à travers diverses activités allant des conférences et des ateliers jusqu'une compétition CTF « Capture The Flag » ou les équipes participantes seront amener à mettre en pratique leurs compétences en matière de cybersécurité pour résoudre des challenges.

Les sujets qui seront abordé concernent la cryptographie, la sécurité du Web, le Bash scripting, le reverse engineering et l'exploitation binaire.

Reference	ANPT-2021-BV-06
Titre	Bulletin de veille N°06
Date de version	30 juin 2021
Contact	ssi@anpt.dz