BULLETIN DE VEILLE N°07

ANPT-2021-BV-07

« One single vulnerability is all an attacker needs. » *-Window Snyder-*

juillet 2021

Alertes de sécurité

DELL

Mise à jour de sécurité de Dell WMS

06 Juillet 2021

Dell a corrigé les vulnérabilités CVE-2021-21587 (CVSS 5.3) et CVE-2021-21586 (CVSS 8.1), dans les versions intérieures à 3.3 de Wyse Management Suite (WMS).

Selon l'équipe, CVE-2021-21587 peut être exploité par un attaquant local non authentifié afin d'obtenir les chemins des fichiers et des dossiers.

La seconde vulnérabilité (CVE-2021-21586) est une vulnérabilité de traversée de chemin absolu qui permet à un utilisateur malveillant authentifié à distance de lire des fichiers arbitraires sur le système.

Les utilisateurs de WMS sont invités à mettre à jour le logiciel.

Source : *https://dell.to/3wZ2G4l*

Microsoft

Plusieurs vulnérabilités dans les systèmes Windows

01-26 Juillet 2021

Microsoft a fait face à trois problèmes de sécurité majeur durent ce mois. Un de ces problèmes, nommé "PrintNightmare" (CVE-2021-34527), affecte le service Spooler d'impression de Windows et peut permettre à des acteurs malveillants distants d'exécuter du code arbitraire et de prendre le contrôle de systèmes vulnérables.
La deuxième vulnérabilité, appelé « SeriousSAM » (CVE-2021-36934), est une vulnérabilité d'élévation locale des privilèges qui permet aux utilisateurs ayant des autorisations de bas niveau d'accéder aux fichiers du registre SAM, SYSTEM et SECURITY du système Windows, ce qui leur permet de démasquer le mot de passe d'installation du système d'exploitation et même de décrypter des clés privées.

L'autre problème, baptisé "PetitPotam", peut être exploité pour forcer des serveurs Windows distants, y compris des contrôleurs de domaine, à s'authentifier auprès d'une destination malveillante, permettant ainsi à un adversaire de faire une attaque de relais NTLM et de prendre le contrôle complet d'un domaine Windows.

Des mises à jour pour les vulnérabilités du service Spooler d'impression sont disponibles. Cependant, aucun correctif n'est disponible pour les autres vulnérabilités. Les administrateurs sont donc invités à consulter les avis de sécurité de Windows (seriousSAM, PetitPotam) afin d'atténuer ces derniers.

Sources : *https://bit.ly/370kB00 ; https://bit.ly/3zDeZFr ; https://bit.ly/2UNXrrk*

SonicWall

SonicWall publie les mises à jour de ses produits pour faire face aux attaques ransomwares

15 Juillet 2021

SonicWall a publié une alerte de sécurité urgente avertissant ses clients que certaines de ses appliances VPN sécurisées actuelles et anciennes faisaient l'objet d'une attaque active en exploitant une vulnérabilité d'injection SQL.
"Les organisations qui ne prennent pas les mesures appropriées pour atténuer ces vulnérabilités sur leurs produits des séries SRA et SMA 100 courent un risque imminent d'attaque ciblée par ransomware", selon le rapport de SonicWall.

Les clients sont invités donc à mettre immédiatement à jour le firmware des appareils encore pris en charge et à "déconnecter immédiatement" les anciens produits, notamment les SRA 4600/1600 (EoL 2019), les SRA 4200/1200 (EoL 2016) et les SSL-VPN 200/2000/400 (EoL 2013/2014).

De plus, si le matériel existant ne peut pas être mis à jour vers les versions 9.x ou 10.x du micrologiciel de SonicWall, la société a déclaré qu'une version gratuite de son SMA 500v virtuel est disponible pendant les 108 prochains jours, et qu'elle expirera le 31 octobre.

Source : *https://bit.ly/3i2MH1d*

Palo Alto

Vulnérabilités multiples dans les produits Palo Alto

14 Juillet 2021

Une vulnérabilité d'élévation de privilèges de haute gravité a été découverte dans les produits Cortex XDR et Prisma Cloud Compute de Palo Alto Networks sur les plateformes Windows. Elle permet à un utilisateur local authentifié de Windows d'exécuter des programmes avec les privilèges SYSTEM.

L'exploitation de cette vulnérabilité nécessite que l'utilisateur dispose de privilèges de création de fichiers dans le répertoire racine de Windows (tel que C:\).

L'application des mises à jour est primordiale pour résoudre ce problème.

Source : *https://bit.ly/371ZGts*

Linux

De nouvelles failles dans Linux donnent aux attaquants les plus hauts privilèges du système

10 Juillet 2021

Deux failles de sécurité ont été découvertes dans le système Linux.

La première, identifiée comme CVE-2021-33909, peut être exploitée par des utilisateurs malveillants pour obtenir des privilèges « root ». Elle affecte les installations par défaut d'Ubuntu 20.04, Ubuntu 20.10, Ubuntu 21.04, Debian 11 et Fedora 34 Workstation, ainsi que les versions 6, 7 et 8 de Red Hat Enterprise Linux.

La seconde, nommée CVE-2021-33910, est une vulnérabilité de déni de service, son exploitation par un utilisateur non privilégié peut faire planter systemd et donc l'ensemble du système d'exploitation.

Les correctifs sont disponibles, et donc les utilisateurs sont invités à les appliquer dès que possible.

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

Kaseya

Kaseya corrige les vulnérabilités du logiciel VSA

11 Juillet 2021

L'éditeur de logiciels Kaseya, a déployé des mises à jour urgentes pour remédier à plusieurs vulnérabilités de sécurité critiques dans sa solution Virtual System Administrator (VSA), qui a été utilisée comme point de départ pour cibler 1 500 entreprises dans le monde entier dans le cadre d'une vaste attaque par ransomware.

L'entreprise a livré donc la version 9.5.7a (9.5.7.2994) de VSA avec des correctifs pour trois nouvelles failles de sécurité, y compris :

- CVE-2021-30116 : Fuite d'informations d'identification.
- CVE-2021-30119 : Faille XSS.
- CVE-2021-30120 : Contournement de l'authentification à deux facteurs.

De plus, la dernière version résout également d'autres failles, notamment un bug qui exposait les hachages de mots de passe faibles dans certaines réponses API à des attaques par force brute, ainsi qu'une vulnérabilité qui pouvait permettre le téléchargement non autorisé de fichiers sur le serveur VSA.

Pour plus de sécurité, Kaseya recommande de limiter l'accès à l'interface graphique Web VSA aux adresses IP locales en bloquant le port 443 entrant sur le pare-feu Internet pour les installations sur site.

Kaseya avertit également ses clients que l'installation du correctif obligera tous les utilisateurs à changer obligatoirement leurs mots de passe après la connexion pour répondre aux nouvelles exigences en matière de mots de passe, ajoutant que certaines fonctionnalités ont été remplacées par des alternatives améliorées et que la "version introduit certains défauts fonctionnels qui seront corrigés dans une prochaine version".

Source : *https://bit.ly/3y4fVSX*

Oracle

Oracle Critcal Patch Update

20 Juillet 2021

Oracle a annoncé qu'un total de 342 vulnérabilités est corrigé dans le cadre de son Critical Patch Update (CPU) de juillet 2021.

Sur l'ensemble des vulnérabilités, une cinquantaine est considérée comme étant de gravité critique, la plus grave, nommée CVE-2021-2244 et ayant un score CVSS de 10, est un bug de sécurité dans le produit Essbase Analytic Provider Services d'Oracle Essbase (JAPI) qui pourrait être exploité à distance sans authentification et qui pourrait conduire à la prise de contrôle complète du produit affecté.

Parmi les autres logiciels Oracle ayant reçu des correctifs pour un grand nombre de vulnérabilités, citons Fusion Middleware (48 vulnérabilités dont 35 exploitables à distance sans authentification), MySQL (41 problèmes traités dont 10 exploitables à distance sans authentification), Communications Applications (33 bugs dont 22 exploitables à distance).

Oracle incite ses clients à appliquer les correctifs disponibles dès que possible, car cela permettrait de réduire considérablement la menace que représentent les attaques réussies.

Source: *https://bit.ly/2Vf0JUw*

Moodle

Moodle fait l'objet de plusieurs vulnérabilités

20 Juillet 2021

Plusieurs vulnérabilités ont été découvertes dans Moodle. Leurs exploitations permettent à une personne malveillante à exécuter un code arbitraire, provoquer un déni de service et compromettre l'intégrité des données.

Il est nécessaire donc aux utilisateurs de Moodle de récupérer et d'appliquer les correctifs afin de se protéger

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

Actualité

Le Projet Pegasus

18 juillet 2021

Le Projet Pegasus, le plus grand scandale de sécurité depuis l'affaire Snowden, a fait son retour. Ce spyware, conçu par une entreprise israélienne nommée NSO, a été découvert pour la première fois en août 2016. Il vise les smartphones (IOS/Android) et semble capable d'exécuter du code arbitraire, d'extraire des contacts, des journaux d'appels, des messages, des photos, l'historique de la navigation Web, des paramètres, ainsi que des informations des applications, notamment les applications de communication iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram et Skype, en d'autres termes, il peut disposer d'un contrôle total sur les smartphones.

Les clients de NSO qui ont la licence de ce logiciel s'en servent pour espionner des personnes haut placées dans la politique, la presse, les droits de l'homme ainsi que les activistes. Plusieurs personnalités politiques, cadres, journalistes et citoyens ont été ciblés, notamment en Algérie.

Edward Snowden - qui a révélé le scandale des écoutes de la NSA - après la fuite de 50000 numéros de téléphone ciblés par pegasus a averti : "Si nous ne faisons rien pour arrêter le commerce de ces technologies, nous ne serons pas à 50 000 numéros de téléphone mais bien à 50 millions de cibles, et cela se produira bien plus vite que nous ne pouvons l'imaginer. Nous devons donc mettre un terme à ce commerce, sans pour autant abandonner la recherche, qui peut être utilisée pour rendre nos appareils plus sûrs".

Au début, Pegasus utilisait des attaques de phishing en envoyant un sms ou un email spécifique à la victime contenant un texte qui la tentait de cliquer sur le lien qui menait à l'installation du peagasus. Par la suite, il a été découvert qu'il exploitait des vulnérabilités de type "zero day" dans Whatsapp et iMessage afin de s'installer sans aucune autorisation (zero-clique).

Une autre méthode appelée "injections réseau" consiste à attendre que la cible visite un site Web qui n'est pas entièrement sécurisé. Une fois que c'est fait, le logiciel du groupe NSO peut accéder au téléphone et déclencher une infection. Kaspersky a également déclaré que Pegasus pour Android ne s'appuie pas que sur des vulnérabilités de type "zero-day". Au lieu de cela, il utilise une méthode d'enracinement bien connue appelée Framaroot.

Des chercheurs d'Amnesty International ont mis au point un outil "Le Mobile Verification Toolkit (MVT)" permettant de vérifier si un téléphone a été visé par le logiciel espion. Mais face au manque de clarté relatif à ce logiciel spyware, aucune contre-mesure n'est possible et aucune prévention n'est envisageable, même une réinitialisation d'usine ne permettra pas de se débarrasser de ce logiciel malveillant.

Source : *https://bit.ly/3f3RddJ ; https://bit.ly/3xdUeyA ; https://bit.ly/3BKzG46*

Le mois des Ransomewares

02 Juillet 2021

Ce mois a été témoin d'une croissance des attaques de ransomware, ce qui lui a fait mériter le nom de mois des ransomwares.

La plus grande attaque de ransomware du mois a été celle qui a ciblé le logiciel VSA de Kaseya le 2 juillet par le rançongiciel du groupe Revil. 1500 de ses clients ont été touchés par cette attaque et une rançon de 70 millions de dollars en bitcoins a été exigée. Kaseya a publié plusieurs correctifs depuis l'attaque et finalement, malgré la disparition du groupe Revil le 12 juillet, Kaseya a réussi à résoudre le problème du ransomware le 22 de ce mois (Pour plus de détails, consultez l'article de Kaseya dans la section Alert).

Sonicwall a également été victime d'un ransomware le 15 de ce mois après l'alerte concernant les séries 100 des produits Secure Mobile Access (SMA) et Secure Remote Access (SRA) en fin de vie non corrigés, ce qui a permis aux ransomwares Hello Kitty et Babuk de les compromettre. (Pour plus de détails sont dans la section Alerte).

De même pour Vmware, le 14 juillet, l'hyperviseur ESXi était une cible du ransomware HelloKitty à cause de la vulnérabilité CVE-2021-22000, des traces de tentatives ont été détectées par MalwareHunterTeam avant la production de dégâts. La vulnérabilité a été corrigée par la suite.

Pour en savoir plus sur les ransomewares et sur la procédure à suivre pour les prévenir et s'en protéger, nous vous invitons à consulter la section "Bon à savoir" ci-dessous.

Source *: https://bit.ly/3iUdOuh ; https://bit.ly/3i8Xk2c ; https://bit.ly/3iQsPxf ; https://bit.ly/2TDF3Rr*

Un outil Ransomware Readiness Assessment par CISA

01 Juillet 2021

Suite à la croissance des attaques par ransomwares, l'agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a publié un nouvel module d'auto-évaluation de la sécurité des ransomwares pour l'outil d'évaluation de la cybersécurité (CSET) de l'agence, nommé RRA (Ransomware Readiness Assessment).

L'outil permettra aux organisations d'évaluer plus facilement leur niveau de protection contre les menaces de ransomware et

les aidera à améliorer leur résistance en appliquant les meilleures pratiques.

En outre, l'évaluation de l'état de préparation aux ransomwares (RRA) guide les propriétaires et les exploitants d'actifs à travers un processus systématique d'évaluation de leurs pratiques de sécurité des réseaux de technologie opérationnelle (OT) et de technologie de l'information (IT) contre la menace des ransomwares.

Il fournit également un tableau de bord d'analyse avec des graphiques et des tableaux qui présentent les résultats de l'estimation sous forme résumée et détaillée.

Le CISA suggère aux organisations de télécharger et d'utiliser le CSET Ransomware Readiness Assessment, qui est disponible sur le dépôt Git Hub de l'Agence.

Source : *https://bit.ly/3i7H4yF*

Des applications malveillantes dans Play Store

04 -12 Juillet 2021

Durant ce mois-ci, Google a détecté l'existence d'un grand nombre d'applications contenant des malwares dans Play Store.

Commençant par le 4 Juillet ou 9 applications qui volent les identifications et mots de passes Facebook ont été trouvées avec 5,8 millions d'installations.

Le 7 juillet, 172 applications payantes se présentant comme des applications de crypto monnaies ont été découvertes, 25 parmi eux été sur Play Store. Plus de 93 000 personnes ont achetés ces applications qui n'étaient en fait qu'une arnaque pour gagner de l'argent.

Enfin, le 12 juillet, les chercheurs de Google ont découvert une nouvelle campagne du malware "Joker" qui se fait passer pour un scanner QR. Ce malware comporte des fonctionnalités de spyware et de cheval de Troie.

Ces applications ont été retirées de Play Store.

De plus, dans une tentative d'amélioration de l'intégrité de Play Store, Google imposant de nouvelles restrictions et protections aux comptes des développeurs, en exigeant l'utilisation d'une méthode d'authentification à deux facteurs et la communication des informations d'identification supplémentaires afin de s'assurer que les comptes sont créés par de "vraies personnes".

Source : *https://bit.ly/3zHMs1u ; https://bit.ly/3xau6V7 ; https://bit.ly/375zILk*

Cloud… soyons prêts !

Choisir un seul cloud ou opter pour le multi-cloud ?

L'une des questions importante qu'il faut poser avant de commencer la migration au cloud est de savoir s'il faut adopter un modèle de cloud unique ou multiple.

Un environnement de cloud unique est réalisé en utilisant un seul fournisseur de cloud pour servir toutes les applications ou services que l'organisation décide de migrer vers le cloud. Tandis qu'une approche multi-cloud consiste plutôt à utiliser différents fournisseurs pour répondre à différentes exigences.

Chaque approche présente des avantages ainsi que certains problèmes. Voici quatre facteurs à prendre en considération lors de la prise de cette décision :

- La flexibilité : L'un des principaux avantages d'une stratégie multi-cloud est qu'elle permet de choisir des fournisseurs qui proposent des innovations adaptées aux besoins : un fournisseur peut offrir la meilleure solution pour un service de messagerie, tandis qu'un autre fournisseur peut être plus apte à fournir des environnements de développement et de test par exemple.
- La sécurité : La sécurité est une responsabilité partagée entre le fournisseur et l'organisation. Dans un environnement à nuage unique, cette division est plus facile à gérer que dans les environnements multi-clouds.
- La complexité : L'un des principaux problèmes liés à une stratégie multi-cloud est sa nature complexe qui nécessite une équipe informatique capable de comprendre les nuances des différents fournisseurs de cloud et d'orchestrer les charges de travail entre eux. Ce problème est le plus souvent rencontré lors de la migration des données ou des applications entre les fournisseurs, ce qui introduit une complexité supplémentaire pour les organisations multi-cloud. Une application créée sur et pour être utilisée sur un fournisseur de cloud computing nécessitera des modifications si le besoin se fait sentir de la déplacer vers un autre fournisseur.
- La dépendance : L'approche mono cloud peut donner à un seul fournisseur de cloud plus d'influence sur une organisation. L'utilisation de plusieurs clouds peut réduire la dépendance à l'égard d'un seul fournisseur de cloud.

Source : *https://bit.ly/3rGu85V*

Bon à savoir !

Ransomwares : Risques et bonnes pratiques

Les ransomwares sont un type de logiciels malveillants qui prennent en otage des fichiers et parfois des ordinateurs ou des appareils mobiles entiers. Les pirates exigent ensuite une rançon en échange du rétablissement de l'accès aux fichiers concernés ou de leur décryptage. Les ransomwares peuvent être introduits via différentes manières, notamment par des sites Web frauduleux et non sécurisés, des téléchargements de logiciels et des spams.

Un certain nombre de facteurs peut faire d'une personne ou d'une entreprise la victime d'une attaque par ransomware, parmi eux :

- L'utilisation d'un appareil ou d'un logiciel obsolète.
- L'absence de correctifs des systèmes d'exploitation, navigateurs, logiciel, etc.
- La cybersécurité ne fait pas l'objet d'une attention suffisante et aucun plan concret n'a été mis en place.

Pour réduire la probabilité de se retrouver face à un ordinateur verrouillé ou à un fichier crypté, il est important de se protéger en appliquant les bonnes pratiques suivantes :

- Ne jamais cliquer sur des liens non sécurisés.
- Éviter de divulguer des informations personnelles.
- Ne pas ouvrir les pièces jointes d'un courriel suspect.
- Ne pas utiliser des clés USB inconnues.
- Maintenir les programmes et les systèmes d'exploitation à jour.
- Utiliser uniquement des sources de téléchargement de confiance.
- Utilisez les services VPN sur les réseaux Wi-Fi publics.
- Maintenir un plan de sauvegarde approprié.

Il est indispensable particulièrement pour les entreprises de sensibiliser leurs employés face aux risques qu'ils encourent.

Source *: https://bit.ly/2Wvitvv ; https://bit.ly/3i2ZoZM*

Evènements

Evènements du mois

DIMVA

14-16 Juillet 2021

Online

https://bit.ly/3x7qbZd

La 18ème édition de l'évènement DIMVA (Detection of Intrusions and Malware & Vulnerability Assessment) a été organisée par le groupe de détection et réponse aux intrusions de la German Informatics Society (GI).

L'évènement a duré 3 jours, son objectif était de faire avancer les connaissances dans le domaine de la détection d'intrusion, de la détection de malware et de l'évaluation de vulnérabilité. Plusieurs sujets ont été abordés, tels que le browser fingerprinting dans la sécurité web, l'utilisation de l'IA dans la détection des malwares sur Android et de la réutilisation du code. En outre, des discussions concernant certaines attaques ont eu lieu ainsi qu'une étude prospective sur les formations de sensibilisation au phishing.

Evènements à venir

Cyber Security Boot Camp

05 Août 2021

Online

https://bit.ly/2Vaowoy

SHPE DFW et Splunk se sont associés pour créer ce camp d'entraînement pour le but d'accroître la sensibilisation et la connaissance de la cybersécurité !

Le camp d'entraînement comprendra trois ateliers d'une heure chacun :

- Introduction à la cybersécurité.
- Un perçu de l'industrie
- Les incidents de cybersécurité connus et les méthodes de défense.

Référence	ANPT-2021-BV-07
Titre	Bulletin de veille N°07
Date de version	31 juillet 2021
Contact	ssi@anpt.dz