BULLETIN DE VEILLE N°7

ANPT-2020-BV-07

« En fin de compte, les objectifs sont simples : la sûreté et la sécurité. »
-Jodi Rell-

Juillet 2020

Alertes de sécurité

Microsoft

Une vulnérabilité RCE critique datant de 17 ans a un impact sur les serveurs DNS Windows

14 juillet 2020

Les chercheurs en cybersécurité ont dévoilé une nouvelle vulnérabilité «vermifuge» très critique affectant les versions de Windows Server 2003 à 2019.

La faille référencée CVE-2020- 1350 d'exécution de code à distance vieille de 17 ans, surnommé « **SigRed** » par Check Point, pourrait permettre à un attaquant distant non authentifié d'obtenir des privilèges d'administrateur de domaine sur des serveurs ciblés et de prendre le contrôle complet de l'infrastructure informatique d'une organisation […].

Dans un rapport détaillé, le chercheur a confirmé que la faille est de nature vermifuge, permettant aux attaquants de lancer une attaque qui peut se propager d'un ordinateur vulnérable à un autre sans aucune interaction humaine.

Microsoft, le fabricant de Windows a préparé un correctif pour la vulnérabilité et a entamé son déploiement dans le cadre de son Tuesday patch de juillet. Si le patch n'est pas appliqué, le risque serait une violation complète de l'ensemble du réseau de l'entreprise.

Source : *https://bit.ly/3jAqCp8*

Une vulnérabilité d'élévation de privilèges dans Microsoft Edge

17 juillet 2020

Une vulnérabilité référencée CVE-2020-1341 d'élévation de privilège a été identifiée dans Microsoft Edge (basé sur Chromium). Lors de téléchargement des fichiers DLL, un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait déposer les fichiers DLL sur les machines victimes et obtenir des privilèges élevés.

Pour exploiter la vulnérabilité, l'utilisateur doit accéder à un site Web malveillant conçu pour télécharger un fichier DLL et cliquer sur la page pour lancer le processus. Dans un scénario d'attaque par e-mail, un attaquant pourrait envoyer un e-mail pour tenter de convaincre l'utilisateur d'accéder au site malveillant.

La mise à jour de sécurité corrige la vulnérabilité en introduisant des mesures de sécurité supplémentaires sur Microsoft Edge à travers l'envoi d'un avertissement à l'utilisateur avant de terminer le téléchargement d'un fichier DLL.

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

L'outil wsreset du Windows 10 Store permet aux attaquants de contourner l'antivirus

20 juillet 2020

Une technique qui exploite une vulnérabilité dans Windows 10 Microsoft Store appelée «wsreset.exe» peut contourner la protection antivirus de contournement sur un hôte sans être détectée. Wsreset.exe est un outil de dépannage légitime qui permet aux utilisateurs de diagnostiquer les problèmes avec le Windows Store et de réinitialiser son cache. Des chercheurs ont découvert que wsreset.exe peut être utilisé de manière abusive pour supprimer des fichiers arbitraires [...]. Ce bug permettrait aux attaquants de supprimer des fichiers même s'ils n'ont pas les privilèges requis pour le faire […].

Cette vulnérabilité d'élévation de privilèges identifiée dans l'utilitaire wsreset.exe peut être utilisée à d'autres fins, comme le contournement de l'UAC, comme cela a déjà été démontré par Hashim Jawad en 2019.

Ce ne sont là que quelques exemples d'autorisations non vérifiées sur les fichiers système de base qui peuvent aider les pirates à passer sous le radar tout en compromettant les systèmes.

Source : *https://bit.ly/3g3lckq*

Android

Google corrige des vulnérabilités critiques d'Android

08 juillet 2020

Plusieurs vulnérabilités critiques d'exécution de code à distance ont été corrigées dans Android avec la publication de l'ensemble de correctifs de sécurité datant de juillet 2020, notamment dans le cadre multimédia et composants système.

La plus grave de ces failles affecte le composant système et pourrait permettre à un attaquant d'exécuter du code avec des privilèges élevés, via un fichier spécialement conçu. En fait, Google a corrigé deux failles critiques dans le composant système, l'une affectant Android 8.0 et les versions plus récentes (CVE-2020-0224), et l'autre affectant uniquement Android 10 (CVE-2020-0225). Une troisième concerne un problème de divulgation d'informations de haute gravité (CVE-2020-0107) qui affecte uniquement Android 10.

Veuillez consulter le bulletin publié par Google pour plus de détails.

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

Adobe

Failles critiques d'Adobe Photoshop corrigées dans une mise à jour d'urgence

21 juillet 2020

Adobe a publié une série de correctifs pour des vulnérabilités critiques qui faisaient partie d'une mise à jour d'urgence. Plusieurs des failles critiques, qui sont liées au très populaire logiciel de retouche photo Adobe Photoshop, permettent aux attaquants d'exécuter un code arbitraire sur des appareils Windows ciblés. Les vulnérabilités de Photoshop affectent Photoshop CC 2019 versions 20.0.9 et antérieures et Photoshop 2020 21.2 et antérieures (pour Windows). Les utilisateurs peuvent mettre à jour respectivement vers les versions 20.0.10 et 21.2.1.

Adobe a également publié des correctifs pour une faille de gravité «importante» dans Adobe Reader Mobile pour Android. La vulnérabilité référencée CVE-2020-9663 permet aux utilisateurs d'afficher et de modifier des fichiers PDF à partir de leur smartphone. L'application a un problème de traversée de répertoire permettant la divulgation d'informations dans le contexte de l'utilisateur actuel. Adobe Reader Mobile pour Android, les versions 20.0.1 et antérieures sont concernées. Les utilisateurs peuvent mettre à jour vers la version 20.3 (pour toutes les versions d'Android).

Source : *https://bit.ly/2WLIDr6*

McAfee

McAfee Total Protection corrige trois vulnérabilités d'élévation de privilèges

02 juillet 2020

Trois vulnérabilités référencées CVE-2020-7281, CVE-2020-7282 et CVE-2020-7283 d'élévation de privilèges ont été corrigées dans McAfee.

Les vulnérabilités existent en raison du fait que l'application n'impose pas correctement les restrictions de sécurité dans le traitement des fichiers journaux lors des mises à jour quotidiennes des fichiers DAT.

L'exploitation des vulnérabilités nécessite l'exécution de code sur un système victime. Ce code ou script manipule de manière malveillante des liens symboliques pour rediriger une action de suppression d'un processus privilégié vers un fichier involontaire.

Toutes les versions inférieures à McAfee Total Protection 16.0.R26 sont affectées. Veuillez-vous assurer que vous disposez de la dernière version « 16.0.R26 ».

Source : *https://bit.ly/2D5Blav*

Cisco

Des pirates ont exploité une faille CVE-2020-3452 dans Cisco ASA et FTD

25 juillet 2020

Cisco a corrigé une vulnérabilité de traversée de chemin de haute gravité CVE-2020-3452 avec le logiciel Cisco Adaptive Security Appliance (ASA) et le logiciel Cisco Firepower Threat Defense (FTD). La vulnérabilité permet à un attaquant distant de lancer une attaque de traversée de répertoire qui lui permet de lire des fichiers sensibles sur un système ciblé.

Une exploitation réussie de la vulnérabilité permet à un attaquant d'afficher des fichiers arbitraires dans le système de fichiers des services Web sur le périphérique ciblé.

Cisco a publié des mises à jour logicielles pour corriger la vulnérabilité, les utilisateurs avec les produits concernés sont recommandés de passer à une version récente dès que possible.

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

Apple

Apple émet des dizaines de correctifs pour ces produits

16 juillet 2020

La mise à jour de sécurité inclut des correctifs pour les bugs dans iOS, macOS, tvOS et WatchOS.

Pour iOS et iPadOS, la mise à jour 13.6 inclut des correctifs pour 29 vulnérabilités, impliquant l'exécution de code arbitraire.

Quatre de ces failles d'exécution de code sont exploitées en lisant des fichiers audio corrompus (CVE-2020-9888, CVE-2020-9889, CVE-2020-9890, CVE-2020-9891). L'exécution de code a également été possible en exploitant AVEVideoEncoder (CVE-2020-9907), iAP (CVE-2020-9914), ImageIO (CVE-2020-9936), iOS Kernel (CVE-2020-9923) et Model I / O (CVE-2020-9878). Le moteur de navigateur WebKit a fait l'objet de trois bugs d'exécution de code : CVE-2020-9894 CVE-2020-9893 et CVE-2020-9895. Dans ces cas, l'exécution de code à distance était possible via une page Web empoisonnée. Ces bugs d'exécution de code à distance apparaissent parfois comme des exploits de jailbreak, les pirates utilisant les failles pour lever ou détourner les restrictions de sécurité de l'App Store.

Source : *https://bit.ly/3gjw2Tq*

Actualité

Le réseau social Twitter a confirmé avoir été victime d'une attaque d'ingénierie sociale

19 juillet 2020

La plateforme de réseaux sociaux Twitter a subi l'une des plus graves cyberattaques de son histoire. Des pirates ont violé un certain nombre de comptes de haut niveau, y compris ceux de Barak Obama, du candidat à la présidentielle américaine Joe Biden, du PDG d'Amazon Jeff Bezos, de Bill Gates, d'Elon Musk, Uber et Apple.

Twitter a expliqué avoir été victime d'une «attaque d'ingénierie sociale coordonnée» contre ses employés qui ont donné aux attaquants l'accès à ses outils internes.

Tous les comptes ont été compromis simultanément et les acteurs de la menace les ont utilisés pour promouvoir une arnaque à la crypto-monnaie. Les attaquants ont publié des messages exhortant les abonnés des comptes piratés à envoyer de l'argent à une adresse de portefeuille Bitcoin spécifique pour recevoir des sommes plus importantes.

Les experts ont également remarqué que les attaquants avaient modifié les adresses e-mail associées aux comptes pour retarder la réponse au détournement.

Maintenant, Twitter a fourni une mise à jour sur l'incident de sécurité confirmant que les attaquants ont ciblé certains employés de Twitter via un plan d'ingénierie sociale.

Pour près de huit comptes Twitter ciblés par les pirates, les intrus ont également téléchargé les informations du compte via l'outil « Vos données Twitter » de Twitter .

Source : *https://bit.ly/32XB4Bo*

Une application malveillante espionne et expose des données des utilisateurs

22 juillet 2020

Des centaines d'applications malveillantes sont apparues sur le Google Play Store, déguisées en applications légitimes. En juillet 2020, les chercheurs d'ESET ont trouvé une application de chat basée sur Android qui fonctionnait comme un logiciel espion et ciblait des utilisateurs au Moyen-Orient. Les pirates faisaient de la publicité pour l'application nommée «Welcome Chat» et affirmaient qu'il s'agissait d'une solution de communication sécurisée. Fonctionnant comme un outil d'espionnage, l'application a laissé les données récoltées sur leurs victimes librement disponibles sur Internet […]. L'application manque en sécurité de base, comme le cryptage des données en transit.

L'application *Welcome Chat* surveille les communications de chat de ses utilisateurs en tant que fonctionnalité d'espionnage principale. Comme action complémentaire, elle infiltre les messages SMS envoyés et reçus, l'historique du journal des appels, les photos, les contacts, les appels téléphoniques enregistrés, la localisation GPS de l'appareil et les informations de cette dernière.

Les utilisateurs ne doivent installer aucune application d'une source autre que Google Play Store ou de sources non fiables. Faites attention et soyez vigilant sur les autorisations requises par diverses applications. Exécutez une solution de sécurité réputée sur les appareils pour rechercher les menaces existantes.

Source : *https://bit.ly/32ZnOw3*

ThiefQuest, le logiciel malveillant macOS à évolution rapide

17 juillet 2020

Dès le début du mois de juillet de cette année, les chercheurs ont remarqué un malware émergent surnommé par la plupart ThiefQuest (ou EvilQuest), une menace qui cible les appareils macOS, crypte les fichiers et installe des enregistreurs de frappe dans les systèmes affectés. Il a été trouvé dans des versions piratées de macOS partagées sur des sites torrent populaires. Les développements sur les logiciels malveillants ont été signalés par MalwareBytes, BleepingComputer et les chercheurs en sécurité Dinesh Devadoss, Phil Stokes, Patrick Wardle, et Thomas Reed .

Les rapports susmentionnés indiquent que l'activité de ransomware n'est pas sa principale méthode d'attaque ; il s'agit plutôt d'un geste préventif pour masquer ses autres activités telles que l'exfiltration de fichiers, la communication de commande et de contrôle (C&C) et l'enregistrement de frappe.

De nouvelles variantes améliorées avec des capacités plus fortes et d'autres changements par rapport aux itérations précédentes du malware ont été aussi découvertes par les chercheurs […].

Les équipes de sécurité et les utilisateurs doivent rester vigilants face à ce malware. Pour ce faire, quelques actions sont recommandées :

- Téléchargez les applications uniquement à partir de sources fiables telles que les magasins d'applications officiels ou les centres de téléchargement.
- Dans les e-mails, ne jamais télécharger de pièces jointes ou cliquer sur des liens provenant de sources non fiables.
- Corrigez et mettez à jour le logiciel pour vous assurer que les vulnérabilités sont corrigées.

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

Sécurité des données d'entreprise : il est temps d'inverser l'approche établi

16 juillet 2020

Selon un article publié sur ThreatPost par Rob Juncker, directeur des nouvelles technologies, l'un des plus gros projet en matière de sécurité de

l'information est la protection des données d'entreprise.

Mais la réalité est qu'aujourd'hui, trop d'organisations «font bouillir l'océan » en ce qui concerne leur programme de sécurité des données. En fait, ils ont toute leur approche de la sécurité des données à l'envers, en particulier lorsqu'il s'agit de gérer les risques liés aux données au sein de la main-d'œuvre hautement collaborative et distante d'aujourd'hui.

Lorsque la plupart des organisations prennent des mesures pour protéger leurs données, elles suivent (ou, plus précisément, tentent de suivre) les pratiques habituelles. Ils commencent par essayer d'identifier toutes les données sensibles dont ils disposent dans leurs organisations - toutes les données qui existent sur leurs partages de fichiers réseau internes, sur les points de terminaison, sur des supports amovibles et dans tous leurs services cloud. Ensuite, ils se concentrent sur l'importance des données, c'est-à-dire sur la classification des informations. Les données sont-elles confidentielles ? Relèvent-elles de la propriété intellectuelle ? Sont-elles importantes ? L'étape suivante consiste à déterminer qui a accès aux données de l'organisation. Enfin, ils cherchent à contrôler ou à bloquer lorsque les données quittent l'organisation.

Quelle est la solution alors ?

Pour commencer, nous devons tous reconnaître quelques vérités de base sur les données d'entreprise :

- Toutes les données sont précieuses, pas seulement les données que nous classons.
- Chaque utilisateur - pas seulement les utilisateurs privilégiés - a accès aux données.
- La collaboration est constante, par conséquent, le blocage ne fonctionnera pas.

Compte tenu de ce qui précède, les organisations doivent inverser leur approche de la sécurité des données et s'attaquer d'abord aux données entrantes et sortantes de l'organisation. Il s'agit d'un sous-ensemble beaucoup plus restreint de la quantité totale de données dans une organisation, et une amélioration considérable par rapport au fait de devoir parcourir plus de deux milliards de fichiers en haut de l'entonnoir de données traditionnel. Avec l'entonnoir inversé, nous commençons littéralement avec un ensemble de fichiers beaucoup plus petit chaque jour et pouvons voir s'il s'agit de fichiers qui nécessitent plus d'attention […].

Conclusion : lorsqu'il s'agit de protéger les données d'entreprise, les organisations n'ont pas à faire bouillir l'océan. En fait, ils ne devraient même pas essayer. Ils doivent se concentrer sur un flux de données beaucoup plus petit - le flux dans lequel leurs données circulent réellement.

Source : *https://bit.ly/3hBIr5F*

Les attaquants développent une nouvelle méthode pour échapper à l'analyse par Any.Run Sandbox

17 juillet 2020

Les auteurs de logiciels malveillants mettent en place des mécanismes pour vérifier si leur code malveillant s'exécute dans le service d'analyse des logiciels malveillants Any.Run.

Any.Run est un service d'analyse de logiciels malveillants qui permet aux chercheurs d'analyser le comportement des logiciels toute en sécurité sans mettre en danger leur système.

Lorsqu'un exécutable est fourni à Any.Run, le service crée une machine virtuelle Windows avec un bureau à distance interactif et le fichier est exécuté. Permettant ainsi aux chercheurs d'observer le comportement exécuté par le logiciel malveillant.

Une nouvelle campagne de chevaux de Troie voleurs de mots de passe a été détectée, dans laquelle des scripts PowerShell malveillants sont utilisés pour installer des logiciels malveillants sur des ordinateurs ciblés. Après l'exécution de ce script, deux scripts contenant le code brouillé de la charge utile malveillante seront téléchargés.

Lors de l'exécution du second script, le cheval de Troie AZORult, qui vole les mots de passe, est tenté de se lancer.

S'il détecte que le logiciel malveillant est exécuté sur Any.Run, il arrête l'exécution du logiciel malveillant. Ainsi, il rend la sandbox incapable d'analyser le malware.

Il est à noter que les plateformes sandbox sont devenues les cibles prioritaires des acteurs malveillants, étant la nouvelle manière d'évasion à la détection.

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

Erreur D-Link : clé de chiffrement du firmware exposée dans une image non chiffrée

22 juillet 2020

Les chercheurs en sécurité ont démontré une méthode pour déchiffrer les images de micrologiciels propriétaires intégrées dans les routeurs D-Link.

Les chercheurs ont analysé la dernière version du firmware D-Link (1.11B02) qui a été téléchargé à partir de leur site Web de support et a utilisé le Binwalk pour cette opération.

Des informations précises ont indiqué aux chercheurs que l'image contenait un binaire de micrologiciel non chiffré qu'il pouvait ensuite extraire et analyser pour les clés de déchiffrement stockées. Les résultats obtenus par les chercheurs soulignent que même le cryptage utilisé est fictif et peut même être considéré comme étant une sécurité par l'obscurité du moment qu'il existe des moyens triviaux pour obtenir la clé gardant le secret. Dans le cas de D-Link, même les images des derniers microprogrammes sont ouvertes à l'analyse des chercheurs curieux qui peuvent obtenir des images de microprogrammes plus anciens - à partir du site de D-Link.

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

Le FBI met en garde contre les nouveaux vecteurs d'attaque DDoS : CoAP, WS-DD, ARMS et Jenkins

27 juillet 2020

Le FBI a envoyé une alerte la semaine dernière pour avertir de la découverte de nouveaux protocoles réseau qui ont été utilisés abusivement pour lancer des attaques de déni de service distribué à grande échelle (DDoS).

L'alerte répertorie trois protocoles réseau et une application Web en tant que vecteurs d'attaque DDoS nouvellement découverts. La liste comprend CoAP (Constrained Application Protocol), WS-DD (Web Services Dynamic Discovery), ARMS (Apple Remote Management Service) et le logiciel d'automatisation Web Jenkins. Trois des quatre (CoAP, WS-DD, ARMS) ont déjà été exploités sur la toile pour lancer des attaques DDoS massives, a déclaré le FBI.

Le but de l'alerte est d'avertir les entreprises américaines du danger imminent, afin qu'elles puissent investir dans des systèmes d'atténuation DDoS et créer des partenariats avec leurs fournisseurs d'accès Internet pour répondre rapidement à toute attaque tirant parti de ces nouveaux vecteurs de plus en plus exploités.

À l'heure actuelle, ces quatre nouveaux vecteurs d'attaque DDoS ont été utilisés de manière sporadique, mais les experts du secteur s'attendent à ce qu'ils soient largement utilisés par les services DDoS-for-location.

Source : *https://zd.net/3gdl95W*

7 services VPN ont divulgué des données de plus de 20 millions d'utilisateurs

20 juillet 2020

Sept fournisseurs de réseaux privés virtuels (VPN) qui prétendent ne conserver aucun journal des activités en ligne de leurs utilisateurs ont récemment laissé 1.2 téraoctet de données d'utilisateurs privés exposés à quiconque vient chercher. Les données, trouvées sur un serveur partagé par les services, comprenaient les informations personnellement identifiables (PII) de pas moins de 20 millions d'utilisateurs VPN, ont déclaré des chercheurs de vpnMentor, qui ont découvert la fuite. Outre les détails personnels, qui comprenaient les adresses e-mail et personnelles des utilisateurs, les mots de passe en texte clair et les adresses IP, il a également été constaté que le serveur stockait plusieurs instances de journaux d'activité Internet.

UFO VPN , FAST VPN , FREE VPN , SUPER VPN , Flash VPN , Secure VPN et Rabbit VPN sont tous impliqués dans l'incident […].

Les utilisateurs de l'un de ces sept fournisseurs de VPN seraient bien avisés d'envisager de passer à un autre service et de modifier leurs informations de connexion sur tout autre compte en ligne. Ce rapport ne doit en aucun cas vous décourager d'utiliser un VPN, mais peut plutôt vous rappeler de choisir votre fournisseur VPN avec soin .

Source : *https://bit.ly/3j8T3Y6*

Evènements

Evènements du mois

ICCICS 2020 : Conférence internationale sur l'intelligence informatique et la cybersécurité

30-31 juillet 2020 à Istanbul, Turquie

https://bit.ly/2CYp9bZ

La Conférence internationale sur la recherche est une organisation fédérée qui se consacre à rassembler un nombre important d'événements universitaires divers.

Des chercheurs se sont réunis pour échanger et partager leurs expériences et leurs résultats de recherche sur tous les aspects de l'intelligence computationnelle et de la cybersécurité. Il fournit également une plate-forme interdisciplinaire de premier ordre aux chercheurs, praticiens et éducateurs pour présenter et discuter des innovations, tendances et préoccupations les plus récentes, ainsi que des défis pratiques rencontrés et des solutions adoptées dans les domaines de l'intelligence informatique et de la cybersécurité.

BSC : Atelier international sur les blockchains et les contrats intelligents

6-8 juillet 2020, Paris, France

https://bit.ly/2CYNe2a

Dans sa troisième édition, l'atelier international est de retour sur les chaînes de blocs et les contrats intelligents, et celui-ci s'est tenu en marge de la 11e conférence internationale de l'IFIP sur les nouvelles technologies, la mobilité et sécurité (NTMS). La blockchain est récemment apparue comme une technologie de rupture susceptible de révolutionner nos sociétés et l'économie mondiale, avec des applications dans des secteurs clés tels que la finance, l'énergie, l'assurance, la mobilité, la santé et la logistique.

Les articles acceptés et présentés seront publiés dans les actes de la conférence et soumis à l'IEEE Xplore®, à la bibliothèque numérique de l'IFIP ainsi qu'à d'autres bases de données d'analyse et d'indexation (A&I).

Reference	ANPT-2020-BV-07
Titre	Bulletin de veille N°7
Date de version	31 Juillet 2020
Contact	ssi@anpt.dz