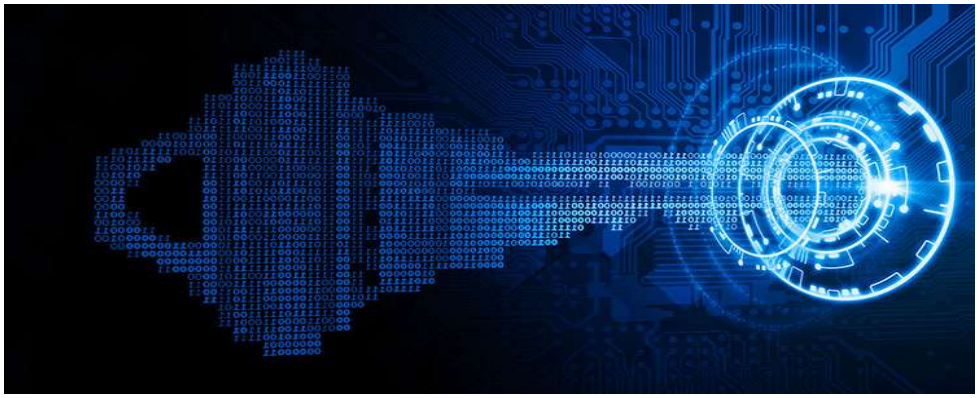


BULLETIN DE VEILLE N°1

ANPT-2021-BV-01

« La sécurité est une culture dont l'entreprise doit faire partie. »

- Britney Hommertzheim -

Janvier 2021

Alertes de sécurité

Microsoft

Des experts détaillent une vulnérabilité récente de Windows exploitable à distance

23 janvier 2021

La faille référencée CVE-2021-1678 a été décrite par Microsoft comme un contournement de la fonctionnalité de sécurité NT LAN Manager (NTLM), toutes les versions de Windows sont affectées, à savoir, Windows Server, Server 2012 R2, Server 2008, Server 2016, Server 2019, RT 8.1, 8.1, 7 et 10.

Selon les chercheurs de Crowdstrike, le bug de sécurité, s'il n'est pas corrigé, pourrait permettre à un acteur malveillant d'exécuter du code à distance via un relais NTLM.

Les exploits réussis pourraient également permettre à un adversaire d'exécuter du code à distance sur une machine Windows ou de se déplacer latéralement sur le réseau vers des systèmes critiques tels que des serveurs hébergeant des contrôleurs de domaine en réutilisant les informations d'identification NTLM dirigées vers le serveur compromis.

La mise à jour de Windows corrige cette vulnérabilité en augmentant le niveau d'authentification RPC et en introduisant une nouvelle stratégie et une nouvelle clé de registre pour permettre aux clients d'activer ou de désactiver le mode d'application côté serveur pour augmenter le niveau d'authentification

Source *: http://bit.ly/36vMbdB*

Microsoft corrige un zero-day dans le Patch Tuesday de Janvier 2021

12 janvier 2020

Dans les mises à jour de ce mois-ci, Microsoft a corrigé un total de 83 vulnérabilités sur une large gamme de produits, y compris son système d'exploitation Windows, ses produits cloud, ses outils de développement et ses serveurs d'entreprise.

Le patch a inclus une vulnérabilité zero-day dans l'antivirus Microsoft Defender, qui, selon Microsoft, a été exploitée avant la publication des correctifs.

La vulnérabilité référencée CVE-2021-1647 a été décrite comme un bug d'exécution de code à distance (RCE) qui permettrait aux acteurs malveillant d'exécuter du code sur des appareils vulnérables sur lesquels Defender est installé.

En plus du Defender zero-day, Microsoft a également corrigé une faille de sécurité dans le service Windows *splwow64* qui pourrait être utilisée abusivement pour élever les privilèges.

Il est recommandé aux administrateurs système de réviser et d'appliquer les correctifs sur l'ensemble des systèmes.

Source *: http://zd.net/3pjm5tL*

Windows 10 fait face à une nouvelle faille de sécurité zero-day

14 janvier 2021

Windows 10 abrite une nouvelle faille de sécurité zero day.

En effet, il est possible de corrompre un disque dur à structure de fichiers NFTS au moyen d'une règle de commande d'une seule ligne. Il s'agit de quelque chose qu'une personne mal intentionnée peut dissimuler dans un raccourci, un fichier zip ou ailleurs et qui ne demande pas de droits d'administration pour être exécuté. Il en résulte qu'une mini-icône manipulée sur le bureau suffit pour exécuter l'action.

Le bug se situerait dans Windows 10 depuis la version build 1803, qui circule depuis avril 2018. Sur slashdot, certains utilisateurs prétendent qu'on peut même en abuser sur un système plus ancien tel Windows XP.

Microsoft a prévu de corriger l'erreur étrange dans les plus brefs délais.

Source *: http://bit.ly/3iLoEm9*

DNS

7 vulnérabilités dans les logiciels de transfert DNS populaires ouvrent la porte à une gamme d'attaques

23 janvier 2021

La faille d'exécution de code à distance, référencée CVE-2020-17530 peut être déclenchée lorsqu'un acteur malintentionné envoie une expression OGNL (Object-Graph Navigation Language) malveillante qui peut entraîner une exécution de code à distance dans le contexte de l'application affectée.

Selon les privilèges associés à l'application affectée, un attaquant pourrait effectuer plusieurs activités malveillantes, telles que l'installation d'applications ; modifier ou supprimer des données, ou créer de nouveaux comptes administrateur.

La faille affectait Struts 2.0.0 à Struts 2.5.25 et a été corrigée dans la version 2.5.26.

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

Linux

Un bug dans Sudo vieux de 10 ans permettrait l'élévation de privilèges

27 Janvier 2021

Une vulnérabilité majeure affectant une grande partie de l'écosystème Linux a été corrigée dans Sudo, une application qui permet aux administrateurs de déléguer un accès limité au niveau d'accès Root à d'autres utilisateurs.

La vulnérabilité, identifiée CVE-2021-3156 et plus communément connue sous le nom de "Baron Samedit", a été découverte par la société d'audit de sécurité Qualys il y a deux semaines et corrigée plus tôt dans la journée avec la sortie de Sudo v1.9.5p2.

Alors que deux autres failles de sécurité dans Sudo ont été révélées au cours des deux dernières années, celle révélée dernièrement est considérée comme la plus dangereuse des trois.

Selon Qualys, la faille affecte toutes les installations Sudo où le fichier sudoers (/etc/sudoers) est présent – ce qui se trouve généralement dans la plupart des installations Linux+Sudo par défaut. Pour aggraver les choses, la vulnérabilité est présente depuis longtemps. Selon Qualys, elle a été introduite dans le code de Sudo en juillet 2011, et affecte toutes les versions de Sudo publiées au cours des 10 dernières années.

Qualys précise que si les opérateurs de botnet utilisent des attaques de force brute pour prendre le contrôle de comptes de service de bas niveau, la vulnérabilité pourrait être exploitée dans une deuxième phase d'une attaque pour aider les intrus à accéder facilement au root et prendre le contrôle de l'appareil piraté.

La mise à jour de Sudo doit être appliquée dès que possible pour éviter de mauvaises surprises de la part des opérateurs de botnet ou d'employés malveillants.

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

Android

Android : 41 failles, dont 4 critiques, corrigées en janvier 2021

5 Janvier 2021

Google a dévoilé un nouveau correctif de sécurité pour Android qui concerne 41 vulnérabilités. En effet, le nouveau bulletin de sécurité pour le mois de janvier a été publié en début du mois par la firme de Mountain View, offrant ainsi un aperçu des correctifs de Janvier.

Au menu de cette rentrée, on peut dénombrer pas moins de 41 vulnérabilités. Elles ne sont pas toutes logées à la même enseigne : la grande majorité de ces brèches (36) sont qualifiées de « sérieuses » dans le document transmis par Google, c'est-à-dire le deuxième niveau le plus élevé sur une échelle de gravité qui en compte trois. Le reste se partage entre 4 failles jugées « critiques » et une « modérée ».

Selon Google, le plus grave de ces problèmes est une faille de sécurité critique située dans le composant Système. La brèche pourrait permettre à un attaquant distant et utilisant une transmission spécialement conçue pour cela d'exécuter un code malveillant en profitant de privilèges particuliers. La bonne nouvelle, vu les conditions requises, est qu'il ne paraît pas évident de pouvoir exploiter cette vulnérabilité.

La mise à jour cible les smartphones équipés des quatre dernières versions d'Android (8, 9, 10 et 11), qui sont respectivement sorties en 2017, 2018, 2019 et 2020. Toutes les failles ne concernent pas toutes les branches d'Android. Certaines par exemple sont exclusives à la 11, qui est disponible depuis décembre dernier. C'est d'ailleurs le cas de trois vulnérabilités ayant trait au même composant (Framework) dans Android.

Source*: https://bit.ly/3cm4iOZ*

Apple

iOS 14.4 a corrigé trois grandes failles exploitées activement

26 Janvier 2021

iOS 14.4, disponible dans sa version finale, comprend des nouveautés mais aussi des correctifs pour des failles. Deux en particulier sont décrites par Apple dans cette fiche comme étant particulièrement redoutables : le constructeur explique en effet que ces vulnérabilités « peuvent être exploitées activement ». Pour le dire autrement : si votre iPhone ou votre iPad est sous iOS 14.3, hâtez-vous d'appliquer la mise à jour qui corrige ces vulnérabilités.

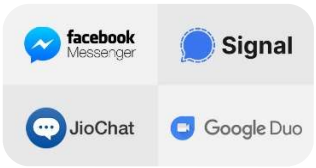
Ces failles touchent le noyau d'iOS ainsi que WebKit. La première permet à une application d'élever ses privilèges et ainsi, pouvoir effectuer des tâches qui lui sont normalement interdites. Les deux autres autorisent l'exécution de code à distance via WebKit. Dans les deux cas, Apple est au courant et annonce des détails supplémentaires à venir.

Source*: https://bit.ly/3r8d9Ip*

Actualité

Les vulnérabilités de Signal, Google Duo et FB Messenger ont permis l'écoute clandestine

20 janvier 2021



Des vulnérabilités ont été révélées dans plusieurs applications de visioconférence et de messagerie qui pouvaient permettre aux utilisateurs malveillants et aux acteurs de la menace d'écouter sans être détectés.

Tout part d'un bug sur FaceTime Video repéré en 2019. Cette faille permettait à un pirate d'espionner les utilisateurs d'iPhone, sans que ces derniers n'aient besoin de décrocher. En outre, un attaquant était également en mesure d'afficher le menu des options et s'ajouter à une conversation de groupe, à l'insu des utilisateurs.

Après plusieurs mois d'analyses approfondies, la chercheuse en sécurité informatique a effectivement déniché plusieurs vulnérabilités de ce type dans Signal, JioChat, Mocha, Facebook Messenger ou encore Google Duo. Voici ce que permettaient ces failles :

- Signal : Une faille dans l'application Android de Signal permettait à un attaquant d'entendre l'environnement du destinataire
- JioChat et Mocha : possibilité pour un attaquant de forcer l'appareil cible à envoyer des flux audio et vidéo sans le consentement de l'utilisateur. Cette vulnérabilité provenait du fait que la connexion peer-to-peer avait été établie avant même que le destinataire ne réponde à l'appel
- Facebook Messenger : Possibilité pour un attaquant connecté à l'appli de lancer simultanément un appel et envoyer un message vérolé à une cible connectée à la fois à l'application mobile et à un autre support (la version Web de Messenger par exemple) et de recevoir l'audio de l'appareil appelé
- Google Duo : Une situation de compétition (il s'agit d'une situation caractérisée par un résultat différent selon l'ordre dans lequel agissent les acteurs du système en informatique) entre la désactivation de la vidéo et la mise en place de la connexion, qui dans certaines situations, pouvait entraîner la fuite de paquets vidéo après plusieurs appels sans réponse.

Toutes ces failles ont été corrigées par les développeurs respectifs de ces applications

Source : *http://bit.ly/3tb9dse*

FreakOut ! Attaque de botnet en cours exploitant des vulnérabilités Linux récentes

19 janvier 2021

Une campagne de malwares en cours a été découverte exploitant les vulnérabilités récemment révélées dans les appareils Linux pour coopter les systèmes dans un botnet IRC afin de lancer des attaques de déni de service distribué (DDoS) et extraire la cryptomonnaie Monero.

Les attaques impliquent une nouvelle variante de malware appelée «FreakOut» qui exploite les failles nouvellement corrigées dans TerraMaster, Laminas Project (anciennement Zend Framework) et Liferay Portal, selon la nouvelle analyse de Check Point Research.

Les chercheurs ont déclaré les failles - CVE-2020-28188, CVE-2021-3007, et CVE-2020-7961 – qui ont été utilisées pour injecter et exécuter des commandes malveillantes dans le serveur.

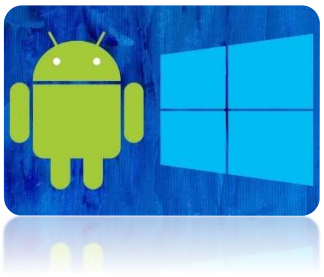
Il a été recommandé aux utilisateurs de mettre à niveau vers Liferay Portal 7.2 CE GA2 (7.2.1) ou version ultérieure et laminas-http 2.14.2 pour atténuer le risque associé aux failles.

"Le fait que certaines des vulnérabilités exploitées viennent juste d'être publiées nous fournit à tous un bon exemple pour souligner l'importance de sécuriser votre réseau en permanence avec les derniers correctifs et mises à jour."

Source : *http://bit.ly/3onZOdh*

Google : l'attaquant a probablement eu accès aux vulnérabilités zero-day d'Android

13 janvier 2021



Le projet Zero de Google a présenté une série en six parties qui propose une analyse de quatre vulnérabilités zero-day sur Windows et Chrome, ainsi que des exploits Android connus lors des recherches approfondies de l'équipe l'année dernière.

Dans un article de blog, l'équipe a déclaré qu'elle avait découvert les vulnérabilités après avoir découvert une attaque de 'watering hole' au premier trimestre 2020 effectuée par un acteur hautement sophistiqué. Les chercheurs ont déclaré avoir découvert deux serveurs offrant différentes chaînes d'exploitation. Un serveur ciblait les utilisateurs Windows, l'autre ciblait Android.

Les quatre zero-day CVE-2020-6418 , CVE-2020-0938, CVE-2020-1020 et CVE-2020-1027 découverts par Project Zero ont été corrigés par les fournisseurs appropriés.

Hank Schless, directeur principal des solutions de sécurité chez Lookout a déclaré que la découverte par Project Zero illustre que les acteurs de la menace considèrent les ordinateurs et les appareils mobiles comme des cibles tout aussi précieuses. Et à mesure que la société dépend de plus en plus d'Android et d'iOS, les appareils mobiles deviennent des cibles aussi précieuses que les ordinateurs portables et les ordinateurs de bureau.

Source : *http://bit.ly/3mAdbWF*

Les serveurs Windows RDP peuvent être exploités dans les attaques DDoS

22 janvier 2021

Les chercheurs de Netscout ont identifié plus de 14 000 serveurs existants qui peuvent être exploités par les attaquants pour inonder de trafic les réseaux des organisations.

Les cybercriminels peuvent exploiter le protocole RDP (Microsoft Remote Desktop Protocol) comme un outil puissant pour amplifier le déni de service distribué (attaques DDoS), selon de nouvelles recherches.

Cependant, tous les serveurs RDP ne peuvent pas être utilisés de cette manière. Cela n'est possible que lorsque le service est activé sur le port 3389/UDP ou le port 3389/TCP, ont déclaré les chercheurs.

Pour atténuer l'utilisation de RDP pour amplifier les attaques DDoS et leur impact associé, les chercheurs ont fait un certain nombre de suggestions aux administrateurs système Windows. Tout d'abord, ils devraient déployer des serveurs Windows RDP derrière des concentrateurs VPN. Si cette atténuation n'est pas possible, ils ont «fortement recommandé» qu'au moins, les administrateurs système désactivent RDP via le port UDP 3389.

Source : *http://bit.ly/3t1k2wL*

Intel dévoile des processeurs anti-ransomware

15 janvier 2021

Intel a dévoilé de nouvelles fonctionnalités anti-ransomware pour sa 11ème génération de processeurs Core ™ vPro ™.

Les nouveaux processeurs, annoncés par Intel lors de la conférence CES, fournissent deux améliorations supplémentaires aux produits de sécurité existants : l'accès aux données au niveau du processeur pour déterminer les attaques de ransomware en cours et l'utilisation de GPU pour l'apprentissage automatique pour renforcer les défenses.

Alors que les responsables de la sécurité de l'information constataient des améliorations de performances grâce à la mise à niveau des puces des ordinateurs d'extrémité, l'un des objectifs du projet est de fournir les avantages de la sécurité sans aucune action supplémentaire de la part des défenseurs.

Cybereason s'est déjà engagé à être parmi les premiers fournisseurs de sécurité à utiliser la technologie. Le directeur de la technologie et co-fondateur Yonatan Striem Amit s'attend à ce que l'entreprise soit en mesure d'utiliser les nouvelles capacités au cours du premier semestre 2021.

Source : *http://zd.net/3pgqldl*

Les logiciels malveillants utilisent le WiFi BSSID pour l'identification des victimes

4 Janvier 2021

Les opérateurs de logiciels malveillants qui souhaitent connaître l'emplacement des victimes qu'ils infectent s'appuient généralement sur une technique simple où ils saisissent l'adresse IP de la victime et la comparent à une base de données IP à géo telle que GeoIP de MaxMind pour obtenir la localisation géographique approximative de la victime.

Cependant, Xavier Mertens, chercheur en sécurité au SANS Internet Storm Center, a déclaré avoir découvert une nouvelle souche de malware utilisant une deuxième technique en plus de la première. Cette deuxième technique repose sur la saisie du BSSID de l'utilisateur infecté. Connu sous le nom d '«identificateur d'ensemble de services de base», le BSSID est essentiellement l'adresse physique MAC du routeur sans fil ou du point d'accès que l'utilisateur utilise pour se connecter via WiFi. Mertens a déclaré que le logiciel malveillant qu'il avait découvert collectait le BSSID, puis le comparait à une base de données BSSID-to-geo gratuite gérée par Alexander Mylnikov. La vérification du BSSID par rapport à la base de données de Mylnikov permettrait au malware de déterminer efficacement l'emplacement géographique physique du point d'accès WiFi que la victime utilisait pour accéder à Internet, ce qui est un moyen beaucoup plus précis de découvrir la position géographique d'une victime.

Source : *https://zd.net/3t4tnnx*

RGPD : En 2020, le montant total des sanctions s'est élevé à 171 millions d'euros, l'Italie en tête

6 Janvier 2021

La France est en sixième position dans le classement des pays qui ont infligé le plus d'amendes au titre du RGPD, avec un total de trois millions d'euros. A la première place se trouve l'Italie qui a prononcé 58,16 millions d'euros de sanctions résultant de 34 infractions. Alors qu'elle est le centre névralgique de la protection des données, l'Irlande est dernière.

Le montant total des sanctions infligées pour violation du Règlement général sur la protection des données (RGDP) est de 171,3 millions d'euros en 2020, d'après le média britannique Finbold. C'est plus qu'entre mai 2018, date d'entrée en vigueur du texte, et janvier 2020. Durant cette période, 114 millions d'euros d'amendes ont été comptabilisées.

Fin janvier dernier, l'autorité de surveillance italienne a par exemple épinglé Eni Gas et Luce (Egl), un fournisseur italien d'électricité et de gaz, en le sanctionnant d'une amende de 11,5 millions d'euros pour marketing illicite.

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

Evènements

Evènements du mois

FloCon 2021

12-15 Janvier 2021, En ligne

https://bit.ly/3cosWOT

FloCon a fourni un forum pour explorer l'analyse de données à grande échelle de nouvelle génération à l'appui des opérations de cybersécurité. FloCon s'adresse aux analystes opérationnels, aux développeurs d'outils, aux chercheurs, aux professionnels de la sécurité et à d'autres personnes intéressées par l'application de techniques de pointe pour analyser et visualiser de grands ensembles de données afin de protéger et de défendre les systèmes en réseau.

SANS Cyber Threat Intelligence Summit

21-22 Janvier 2021, virtuel

https://bit.ly/2Yo6kGi

La collecte, la classification et l'exploitation des connaissances sur les adversaires - collectivement connues sous le nom de cyber-renseignements sur les menaces (CTI) – ont conféré aux praticiens de la sécurité une supériorité sur les informations qui sont utilisées pour réduire les chances de succès d'un adversaire. Les intervenants et les défenseurs ont tiré parti de renseignements précis, opportuns et détaillés sur les menaces pour surveiller les attaques nouvelles et en évolution et adapter ultérieurement leur posture de sécurité.

Evènements à venir

Conférence MENA sur la cybersécurité pour les actifs critiques

1 et 2 Février 2021, Dubaï, UAE

https://bit.ly/2MiKu4z

Alors que la géopolitique façonne les perspectives de sécurité de la région, l'appétit croissant pour l'IIoT présente un environnement de risque complexe pour les parties prenantes. Cela a fait de la sécurité des opérations industrielles une place centrale dans la C-suite. Dans cet esprit, l'agenda de la conférence 2021 se concentrera sur le déchiffrement du code de sécurité dans les environnements OT. Cela comprend la résolution des problèmes de cybersécurité de l'IIoT ainsi que la fourniture d'outils pour les stratégies intégrées IT / OT.

Reference	ANPT-2021-BV-01
Titre	Bulletin de veille N°1
Date de version	31 Janvier 2021
Contact	ssi@anpt.dz