BULLETIN DE VEILLE N°3

ANPT-2020-BV-03

« La menace est un miroir des failles de sécurité. La cyber-menace est principalement le reflet de nos faiblesses. » - Stephane Nappo-

Mars 2020

Alertes de sécurité

Microsoft

Le correctif Microsoft de mars corrige 115 vulnérabilités

10 mars 2020

Microsoft a publié des correctifs pour 115 vulnérabilités dans les produits Microsoft. Parmi les failles les plus critiques, la vulnérabilité référencée CVE-2020-0872 d'exécution de code à distance dans « Application Inspector ». Deux autres vulnérabilités référencées CVE-2020-0684 et CVE-2020-0852 ont été corrigées, ce qui pourrait permettre aux attaquants de créer des fichiers *.LNK* ou des documents Word spécialement conçus pouvant exécuter le code une fois ouverts.

Pour accéder à la description complète de chaque vulnérabilité et des systèmes qu'elle affecte, vous pouvez consulter le rapport complet ici . Il est fortement recommandé d'installer les mises à jour de sécurité dès que possible pour se protéger contre les risques de sécurité connus.

***Source** : http://bit.ly/38RWQpn*

Explication de la vulnérabilité de Microsoft SMBv3.11 et du correctif CVE-2020–0796

12 mars 2020

Un correctif (KB4551762) de la dernière faille référencée CVE-2020-0796 (SMBGhost) a été publié par Microsoft. Ce correctif concerne la vulnérabilité qui a touché le **protocole SMBv3** dans le système Windows 10, les versions 1903 et 1909, ainsi que le Windows Server 2019, versions 1903 et 1909.

La faille permet aux attaquants d'être connectés à distance aux systèmes ayant un service SMB activé, mais aussi d'exécuter un code malveillant ayant les privilèges SYSTEM. Ceci engendre une possibilité de contrôler à distance l'ensemble des systèmes vulnérables.

Un avis de sécurité a été publié à l'intention des utilisateurs n'arrivant pas à installer le correctif immédiatement.

***Source** : http://bit.ly/2x0nz60; **CVE détail** : http://bit.ly/38PQ1Vu*

Microsoft publie un avis pour Windows Zero-Day

23 mars 2020

Microsoft a publié le 23 mars un avis pour informer les utilisateurs des attaques actives ciblant des failles non corrigées dans la bibliothèque Adobe Type Manager. Les vulnérabilités affectent toutes les versions prises en charge de Windows.

Il existe deux vulnérabilités d'exécution de code à distance dans Microsoft Windows lorsque la bibliothèque Windows Adobe Type Manager ne gère pas correctement une police multi-maître spécialement conçue pour le format PostScript Adobe Type 1.

Il existe plusieurs façons pour un attaquant d'exploiter la vulnérabilité, par exemple en convainquant un utilisateur d'ouvrir un document spécialement conçu ou de le visualiser dans le volet Aperçu de Windows. Veilliez consulter l'avis pour appliquer les mesures de contournement, en attendant que Microsoft publie les mises à jour qui corrigent les vulnérabilités de sécurité qui sont généralement publiées dans la mise à jour habituelle qui a lieu le deuxième mardi de chaque mois.

***Source** : https://bit.ly/2J7GwXc*

Windows 10 : le bug de Windows Defender ignore les fichiers lors des scans

22 mars 2020

Dernièrement, les utilisateurs de Windows 10 ont remarqué que des fichiers sont ignorés lors de l'analyse de Windows Defender à cause d'un paramètre d'exclusion ou d'analyse réseau configuré.

Néanmoins, ces utilisateurs n'ont pas d'exclusion configurée dans les préférences de Windows Defender. Même lorsque l'utilisateur réalise « une analyse rapide » ou encore une analyse complète en utilisant Windows Defender, il reçoit une notification du Centre d'action Windows 10 qui indique que l'analyse n'a pas été faite pour certains éléments.

Nous ne savons pas quand exactement ce bug a vu le jour, mais d'après plusieurs rapports, [1 , 2], ceci a commencé vers le 10 mars 2020, coïncidant avec le patch de mardi.

Ce bug doit encore être analysé et aucune réponse n'est encore publiée par Microsoft à ce sujet.

Source : *https://bit.ly/33JiafK*

Apple

Vulnérabilité de contournement VPN dans Apple iOS

25 mars 2020

Une vulnérabilité a été découverte dans la version iOS 13.4 d'Apple qui empêche les VPN de crypter tout le trafic. Lorsqu'une connexion VPN est établie, le système d'exploitation de l'appareil ferme toutes les connexions Internet existantes, puis les rétablit via le tunnel VPN. Les connexions qui sont déjà en cours d'exécution lorsque vous vous connectez au VPN peuvent continuer indéfiniment en dehors du tunnel VPN.

Une solution de contournement consiste à activer le mode avion après connexion au serveur VPN, puis le désactiver. Apple recommande également d'utiliser Always-on VPN pour atténuer ce problème. Cette méthode nécessite l'utilisation de la gestion des appareils , donc malheureusement elle n'atténue pas le problème pour les applications tierces telles que ProtonVPN. Jusqu'à ce qu'une mise à jour soit disponible auprès d'Apple, nous recommandons les solutions de contournement ci-dessus.

Source : *https://bit.ly/2Jol6FB*

Google

Google Security Update a corrigé plusieurs vulnérabilités de gravité élevée dans Chrome

23 mars 2020

Google a publié Chrome 80.0.3987.149, une mise à jour de canal stable pour Windows, Mac et Linux avec les correctifs de plusieurs vulnérabilités de gravité élevée.

Google a résolu 13 bugs dans divers composants Chrome tels que WebGL , les médias et l'audio signalés par des chercheurs externes en sécurité. Pour avoir plus de détails sur les différentes vulnérabilités veuillez consulter l'avis de Google.

Afin d'appliquer les mises à jour :

1. Ouvrir le navigateur Chrome
2. Se diriger vers les paramètres
3. Développer l'aide
4. À propos de Google Chrome
5. Le navigateur traitera la mise à jour

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

Android

Google corrige une faille dangereuse

04 mars 2020

Google a révélé une vulnérabilité grave affectant des dizaines de modèles d'appareils Android de milieu de gamme fonctionnant sur des puces de MediaTek. Des applications Android malveillantes exploitent la faille depuis au moins janvier 2020.

La faille d'élévation de privilèges, identifiée comme CVE-2020-0069, est divulguée dans le bulletin Android de mars 2020 de Google et affecte le pilote MediaTek Command Queue.

La partie dangereuse de ce bogue est qu'un exploit subsistait depuis près d'un an appelé «MediaTek-su», qui permet un accès root temporaire sur un grand nombre de puces MediaTek.

Un développeur qui s'appelle «diplomatique» a utilisé les forums des développeurs XDA pour partager un script que les utilisateurs peuvent exécuter pour accéder au super-utilisateur (su).

Source : *https://zd.net/3cCd9dk*

Apache

Apache Tomcat affecté par un bug Ghostcat

02 mars 2020

Une vulnérabilité à haut risque appelée Ghostcat a affecté les serveurs Apache Tomcat vendus durant les 13 dernières années. La vulnérabilité référencée CVE-2020-1938 a été découverte par une société chinoise de cyber sécurité Chaitin Tech. C'est une faille qui provient du protocole Tomcat AJP. Le connecteur AJP de Tomcat est activé par défaut sur tous les serveurs Tomcat et écoute sur le port 8009 du serveur.

La vulnérabilité GhostCat peut permettre aux attaquants distants de lire le contenu de n'importe quel fichier sur un serveur web ou bien sur un conteneur de servlet vulnérables et d'obtenir un fichier de configuration ou encore un code source sensible. Il est également possible d'exploiter la faille afin d'exécuter du code dans le cas d'une autorisation de téléchargement de fichiers par le serveur.

L'ensemble des branches Tomcat 6.x, 7.x, 8.x, et 9.x sont affectées par la vulnérabilité GhostCat. Les correctifs des branches Tomcat 7.x, Tomcat 8.x et Tomcat 9.x ont été publiés. Une mise à jour de l'outil XRAY a également été publiée par l'équipe Chaitin pour faire une analyse des réseaux cherchant les serveurs TomCat vulnérables.

Il est à noter que des PoC (Proove of Concept) [1 , 2 , 3 , 4 , 5] existent déjà sur GitHub.

Source : *http://bit.ly/3aqqd3e*

Linux

Une faille critique dans démon PPP

05 mars 2020

Découvert par le chercheur en sécurité IOActive Ilja Van Sprundel, le problème critique est une vulnérabilité de débordement de tampon de pile qui existe en raison d'une erreur logique dans l'analyseur de paquets EAP (Extensible Authentication Protocol) du logiciel pppd, une extension qui prend en charge des méthodes d'authentification supplémentaires dans les connexions PPP. La vulnérabilité référencée CVE-2020-8597, peut être exploitée par des attaquants non authentifiés pour exécuter à distance du code arbitraire sur les systèmes affectés et en prendre le contrôle total. Selon le chercheur, les versions 2.4.2 à 2.4.8 du démon de protocole point à point - toutes les versions publiées au cours des 17 dernières années - sont vulnérables à cette nouvelle vulnérabilité d'exécution de code à distance. Les distributions Linux suivantes : Debian, Ubuntu, SUSE Linux, Feutre, NetBSD, Red Hat Enterprise Linux, ont déjà été confirmées comme impactées. D'autres applications sont aussi vulnérables (Cisco CallManager, Produits, TP-LINK, Système

d'exploitation intégré OpenWRT, Produits Synology). Il est conseillé aux utilisateurs des systèmes d'exploitation et des périphériques concernés d'appliquer des correctifs de sécurité dès que possible ou lorsqu'ils seront disponibles.

Source : *http://bit.ly/39xy1Ad*

Vmware

VMware corrige un bug critique dans ces produits

13 mars 2020

VMware a corrigé trois vulnérabilités graves dans ses produits, y compris une faille critique référencée CVE-2020-3947 dans Workstation et Fusion. Une exploitation réussie de ce problème peut entraîner l'exécution de code sur l'hôte ou peut permettre à des attaquants de créer une condition de déni du service vmnetdhcp exécuté sur la machine hôte.

Une autre faille résolue par VMware, référencée CVE-2020-3948, est une vulnérabilité d'élévation de privilèges locale dans Cortado Thinprint. Il s'agit d'une faille très grave qui pourrait être exploitée par un attaquant local disposant d'un accès non administrateur à une machine virtuelle invitée Linux (VM) avec VMware Tools installé pour augmenter les privilèges de root sur la même machine virtuelle.

Les produits affectés sont Workstation 15.x sur n'importe quelle plateforme et Fusion 11.x sur MacOs. Il est recommandé de mettre à niveau Workstation à la version 15.5.2 et Fusion à la version 11.5.2.

Source : *http://bit.ly/2QnTQuv*

Intel

Un bug important affecte les chipsets d'Intel

06 mars 2020

D'après l'entreprise Positive Technologies, le bug qui a récemment affecté les processeurs d'Intel (ayant été corrigé l'an dernier) est plus grave que ce que l'on croyait.

Lorsque la mise à jour de sécurité Intel-SA-00213 a été publiée en mai 2019, la société Intel a corrigé un bug au niveau des processeurs Intel qui a affecté le CSME. La vulnérabilité a été référencée CVE-2019-0090 et a été décrite comme étant un simple bug de firmware permettant aux attaquants qui disposent d'un accès physique au CPU d'avoir plus de privilèges et d'exécuter du code à partir du CSME. Quelques autres technologies telles que Intel TXE (Trusted Execution Engine) et SPS (Server Platform Services) ont également été touchées.

Selon Mark Ermolov, spécialiste en chef de la sécurité des systèmes d'exploitation et du matériel chez Positive Technologies, il est possible d'exploiter ce bug afin de récupérer la clé du chipset qui est en fait la clé cryptographique racine permettant à l'attaquant d'avoir accès à tout ce qui se trouve sur un appareil. Ce bug peut aussi être exploité à travers un « accès local » par un logiciel malveillant sur un appareil, sans disposer obligatoirement d'un accès physique au système. Selon les chercheurs de l'entreprise Positive Technologies, cette vulnérabilité provient de l'absence de protection du microprogramme du CSME sur la ROM d'amorçage au début du démarrage, et ceci permet d'extraire la clé du chipset par de multiples moyens pendant un intervalle de temps court.

Source : *http://bit.ly/2vwzloo*

Intel corrige des défauts dans les pilotes graphiques Windows

11 mars 2020

Intel a publié des mises à jour de sécurité pour corriger 27 vulnérabilités dans le cadre du patch de mars 2020, dix d'entre elles étant des failles de sécurité de haute gravité affectant les pilotes graphiques d'Intel pour Windows et le DSP audio intégré de la technologie Smart Sound Technology dans les processeurs Intel Core et Intel Atom. Les vulnérabilités révélées peuvent permettre à des utilisateurs authentifiés ou privilégiés d'accéder potentiellement à des informations sensibles, de déclencher des états de déni de service et d'augmenter les privilèges via un accès local.

Les problèmes de sécurité corrigés aujourd'hui sont détaillés dans les neuf avis de sécurité publiés par Intel sur son Security Center , la société a fourni des liens de téléchargement pour les mises à jour de sécurité disponibles via les pilotes et le centre de téléchargement de logiciels.

Source : *http://bit.ly/2QoVmfY*

Adobe

Vulnérabilité détectée dans Adobe Flash

11 février 2020

Un avis de cybersécurité a été publié concernant une vulnérabilité référencée CVE-2020-3757 dans Adobe Flash. Une exploitation réussie de cette vulnérabilité pourrait conduire un attaquant à exécuter du code arbitraire dans le contexte de l'application affectée.

Il est recommandé d'installer les mises à jour fournies par Adobe immédiatement.

Systèmes concernés : Adobe Flash Player Desktop Runtime pour Windows et macOS versions antérieures à 32.0.0.321 | Adobe Flash Player Desktop Runtime pour Linux versions antérieures à 32.0.0.314 | Adobe Flash Player pour Google Chrome pour Windows, macOS, Linux et Chrome OS versions antérieures à 32.0 .0.321 | Adobe Flash Player pour Microsoft Edge et Internet | Explorer 11 pour Windows 10 et 8.1 avant 32.0.0.255.

Source : *http://bit.ly/37ACIrq*
Correctifs : *https://adobe.ly/2ua9ZMr*

Actualité

Les attaques par ondes ultrasonores peuvent exploiter la reconnaissance vocale du smartphone

03 mars 2020

Les chercheurs ont découvert une faille de sécurité dans les systèmes de reconnaissance vocale des smartphones en raison de laquelle les ondes ultrasonores peuvent activer Siri et Google Assistant.

Selon des recherches de l'Université de Washington à St. Louis, les ondes ultrasonores peuvent se propager à travers des surfaces solides pour activer les systèmes de reconnaissance vocale dans les téléphones portables. De plus, avec l'ajout de matériel bon marché, un attaquant peut lancer l'attaque pour écouter la réponse du téléphone. L'attaquant peut envoyer des commandes au téléphone pour passer des appels, prendre des images ou lire le contenu de texte, le tout à l'insu du propriétaire du téléphone.

L'équipe de recherche a mis en place une multitude d'expériences sur 17 modèles de téléphones différents, y compris les modèles iPhone, Galaxy et Moto. […]. Des ondes ultrasonores ont traversé le métal, le verre et le bois pendant les expériences. Les chercheurs ont également testé différentes surfaces de table et configurations de téléphones, même à des distances allant jusqu'à 10 mètres.

L'équipe d'experts a suggéré que si nous pouvions différencier le signal reçu par téléphone entre les ondes ultrasonores et les véritables voix humaines, cette situation pourrait être résolue. L'autre façon pourrait être de changer la disposition des téléphones portables, comme l'emplacement du microphone, pour amortir ou supprimer les ondes ultrasonores. Cela pourrait arrêter une «attaque de surf» […].

Source : *http://bit.ly/32QaisM*

Let's Encrypt révoque 3 millions de certificats le 4 mars en raison d'un bug logiciel

04 mars 2020

Let's Encrypt a émis 3 048 289 certificats TLS sans vérifier le champ CAA du domaine demandeur. Plus précisément, le bug a affecté Boulder, le logiciel serveur utilisé par le projet Let's Encrypt pour vérifier les utilisateurs et leurs domaines avant d'émettre un certificat TLS.

Les propriétaires de domaine peuvent ajouter un "champ CAA" aux enregistrements DNS de leur domaine et seule l'autorité de certification répertoriée dans le champ CAA peut émettre un certificat TLS pour ce domaine.

Toutes les autorités de certification - comme Let's Encrypt - doivent suivre la spécification CAA à la lettre conformément à la loi ou s'exposer à de lourdes sanctions de la part des fabricants de navigateurs. Let's Encrypt prévoit de révoquer tous les certificats concernés, à partir de 00h00 UTC, le 4 mars 2020.

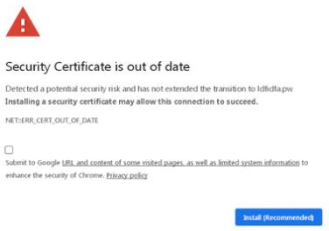
Après cette date, tous les certificats impactés déclencheront des erreurs dans les navigateurs et autres applications. Par conséquent, les propriétaires de domaine devront demander un nouveau certificat TLS et remplacer l'ancien.

Les administrateurs système et les webmasters qui utilisent actuellement des certificats Let's Encrypt pour leurs réseaux et serveurs peuvent consulter une liste des numéros de série des certificats TLS impactés sur cette page , ou ils peuvent visiter le site Web suivant et vérifier si leur certificat a été impacté.

Source : *https://zd.net/3aplUp2*

Les logiciels malveillants se propagent grâce à de fausses alertes de certificats de sécurité

05 mars 2020



Les variantes de logiciels malveillants de porte dérobée et de chevaux de Troie sont distribuées grâce à une nouvelle technique de phishing qui tente d'attirer les victimes en acceptant une «mise à jour» des certificats de sécurité du site Web.

Des chercheurs en cybersécurité de Kaspersky ont signalé que la nouvelle technique avait été repérée sur divers sites Web, allant d'un zoo à un magasin de commerce électronique vendant des pièces de véhicules. Les visiteurs d'un domaine compromis par la campagne reçoivent l'alerte prétendant que le certificat de sécurité du site Web est obsolète, invitant les victimes à installer une « mise à jour du certificat de sécurité » pour continuer. Si la victime choisit de cliquer sur le bouton de mise à jour, le téléchargement d'un fichier, Certificate_Update_v02.2020.exe, est lancé.

Une fois décompressé et installé, l'exécutable fournira l'une des deux variantes de logiciels malveillants à la victime, Mokes ou Buerak […].

Source : *https://zd.net/2IohYsJ*

Rootkit dans le cloud : un groupe de hackers viole les serveurs AWS

03 mars 2020

Un groupe de hackers sophistiqués a piraté des serveurs Amazon Web Services (AWS), mis en place un rootkit qui leur a permis de contrôler à distance les serveurs, puis acheminé les données sensibles vers ses serveurs de commande et de contrôle (C2) à partir d'une gamme de machines Windows et Linux compromises à l'intérieur un centre de données AWS.

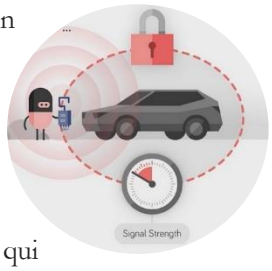
C'est selon un rapport du Sophos britannique publié à la fin de la semaine dernière. Les attaquants ont pu contourner les groupes de sécurité AWS (SG), qui, lorsqu'ils sont correctement configurés, agissent comme un périmètre de sécurité pour les

instances Amazon EC2 associées. La cible non nommée de cette attaque avait correctement réglé ses SG. Mais le système Linux compromis était toujours à l'écoute des connexions entrantes sur les ports 2080/TCP et 2053/TCP : ce qui a finalement déclenché l'intervention de Sophos. Le rapport complet de Sophos sur les techniques utilisées est disponible ici.

Source : *http://bit.ly/32SxSVM*

Les pirates peuvent cloner des millions de clés Toyota, Hyundai et Kia

05 mars 2020



Des chercheurs de la KU Leuven en Belgique et de l'Université de Birmingham au Royaume-Uni ont révélé de nouvelles vulnérabilités qu'ils ont trouvé dans les systèmes de cryptage utilisés par les immobilisateurs, les appareils radio-activés à l'intérieur des voitures qui communiquent à courte distance avec un porte-clés pour déverrouiller l'allumage de la voiture et lui permettre de démarrer. Plus précisément, ils ont trouvé des problèmes dans la façon dont Toyota, Hyundai et Kia implémentent un système de cryptage Texas Instruments appelé DST80. Un pirate qui passe un lecteur / émetteur Proxmark RFID près du porte-clés de toute voiture avec DST80 à l'intérieur peut obtenir suffisamment d'informations pour dériver sa valeur cryptographique secrète. Cela, à son tour, permettrait à l'attaquant d'utiliser le même appareil Proxmark pour usurper l'identité de la clé à l'intérieur de la voiture, désactivant le dispositif d'immobilisation et le laissant démarrer le moteur.

Les chercheurs affirment que les modèles de voitures concernés comprennent les Toyota Camry, Corolla et RAV4 ; les Kia Optima, Soul et Rio ; et les Hyundai I10, I20 et I40 […].

Toyota a répondu dans un communiqué que "la vulnérabilité décrite s'applique aux modèles plus anciens, car les modèles actuels ont une configuration différente." La société a ajouté que "cette vulnérabilité constitue un faible risque pour les clients, car la méthodologie nécessite à la fois l'accès à la clé physique et à un appareil hautement spécialisé qui n'est pas couramment disponible sur le marché". Sur ce point, les chercheurs n'étaient pas d'accord, notant qu'aucune partie de leur recherche ne nécessitait du matériel qui n'était pas facilement disponible […].

Malgré tout, les chercheurs disent qu'ils ont décidé de publier leurs résultats pour révéler l'état réel de la sécurité de l'antidémarrage et permettre aux propriétaires de voitures de décider eux-mêmes si cela suffit.

Source : *http://bit.ly/39MoBkN*

Vulnérabilité zero-day dans les services SaaS exploitée pour lancer des attaques de phishing

05 mars 2020

Les cybercriminels exploitent une vulnérabilité zero-day dans Verisign et plusieurs services SaaS pour enregistrer des domaines et sous-domaines génériques malveillants de premier niveau qui ressemblent à des sites légitimes. Les services SaaS concernés sont Google, Amazon et DigitalOcean. L'objectif est de lancer des attaques de phishing contre des organisations.

Démontrée par Matt Hamilton, chercheur principal en sécurité chez Soluble, la vulnérabilité est similaire à une attaque IDN Homograph et présente les mêmes risques.

Il souligne qu'un attaquant pourrait enregistrer un domaine ou un sous-domaine qui apparaît visuellement identique à son homologue légitime et effectuer des attaques d'ingénierie sociale contre une organisation.

Verisign, le registre faisant autorité pour les domaines .com, .net, .edu et plusieurs autres domaines génériques de premier niveau (gTLD) a corrigé la faille et restreint désormais l'enregistrement des domaines utilisant ces caractères homoglyphes. En outre, il a modifié les règles d'enregistrement des noms de domaine en mettant à jour la table des caractères autorisés dans les domaines nouvellement enregistrés.

Source : *http://bit.ly/2TTXeOI*

Explorer diverses façons dont les pirates traient la peur du COVID-19

13 mars 2020

Les pirates ont l'habitude de saboter et de manipuler les urgences publiques pour leurs propres gains […]. Récemment, les pirates ont lancé plusieurs campagnes d'attaque dans différents pays, profitant de la propagation de la maladie […]. Ils ont été repérés en train de distribuer des chevaux de Troie comme Emotet, AZORult, AgentTesla Keylogger et NanoCore pour voler les informations d'identification des utilisateurs via des campagnes d'attaque sur le thème du coronavirus. Dans un cas, des attaquants ont conçu un e-mail pour attiser la curiosité sur un remède disponible. S'ils souhaitent recevoir de plus amples informations, ils doivent cliquer sur le lien malveillant fourni dans l'e-mail. Une autre méthode d'attaque sophistiquée qui, selon les chercheurs, contenait un document MS Word de l'Organisation mondiale de la santé avec une URL intégrée menant à un faux site Web. De plus, certains attaquants invitent les utilisateurs à télécharger une application pour les tenir informés de la situation. Il affiche simplement une carte de la propagation du COVID-19. Lorsqu'un utilisateur se trouve sur la page, les attaquants tentent de générer un fichier binaire malveillant et de l'installer sur l'ordinateur. Actuellement, cette pratique affecte uniquement les systèmes Windows. Les utilisateurs doivent être vigilants et n'utiliser que les sources fiables.

Source : *http://bit.ly/2Wg0tmo*

Espionnage de millions d'utilisateurs à travers 20 applications mobiles

10 mars 2020

Au minimum 20 applications bloqueurs de publicités et VPN téléchargées 35 millions de fois ont été recensées par le site BuzzFeed News. Selon l'enquête de ce site, ces applications ont été publiées sur Android et iOS dès l'année 2015, et celles-ci font la collecte des données des utilisateurs sans qu'ils le sachent. Ces VPN et bloqueurs de publicité appartiennent à une plateforme d'analytique nommée Sensor Tower. Des données échangées par le smartphone ont été accessibles en utilisant un certificat racine. Sensor Tower a contourné les restrictions pour inciter les utilisateurs à télécharger le certificat à partir du site internet suite à l'installation de l'application.

La société a dissimulé son lien avec les VPN et bloqueurs de publicité aux utilisateurs et les a publié sous d'autres appellations comme Emban Networks ou encore **Gibli Mobile**. Selon le chef analyste mobile de Sensor Tower « Randy Nelson », aucune donnée sensible ou information personnellement identifiable n'a été collectée. La majorité des applications étaient déjà supprimées pour viol des règles d'Apple et de Google. Après que BuzzFeed ait contacté Apple, cette dernière a retiré Adblock Focus de l'App Store, sauf que Luna VPN y est toujours. Concernant Google, le Play Store d'Android détient toujours les applications Luna VPN, Mobile Data et Free and Unlimited VPN. La société enquête toujours sur l'affaire.

Source *: http://bit.ly/38MD0Mk*

La vulnérabilité Kr00k permet aux attaquants de déchiffrer les paquets WiFi

04 mars 2020

Lors de la conférence sur la sécurité RSA 2020 à San Francisco, les chercheurs en sécurité de la société slovaque antivirus ESET ont présenté des détails sur une nouvelle vulnérabilité qui affecte les communications WiFi.

Nommé Kr00k, ce bug peut être exploité par un attaquant pour intercepter et décrypter un certain type de trafic réseau WiFi (s'appuyant sur les connexions WPA2). Selon ESET, Kr00k affecte tous les appareils compatibles WiFi fonctionnant sur des puces Wi-Fi Broadcom et Cypress. Ce sont deux des chipsets WiFi les plus populaires au monde, et ils sont inclus dans de nombreux appareils, allant des ordinateurs portables aux smartphones, et des points d'accès aux haut-parleurs intelligents et autres objets connectés.

Les chercheurs d'ESET ont déclaré avoir testé et confirmé que Kr00k avait un impact sur les appareils d'Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3) et Xiaomi (Redmi), mais aussi des routeurs Asus et Huawei.

Dans un communiqué de presse publié la semaine dernière, ESET estime que plus d'un milliard d'appareils sont vulnérables à Kr00k. Les utilisateurs peuvent vérifier s'ils ont reçu des correctifs Kr00k en vérifiant les journaux des modifications du système d'exploitation / du firmware de leur appareil par rapport à CVE-2019-15126, qui est l'ID unique attribué pour suivre ce bogue. Pour plus de détails techniques cliquer ici.

Source *: http://bit.ly/2QoEDJC*

Evènements

Evènements du mois

Depuis la propagation de la pandémie et l'introduction du coronavirus Covid-19 en Algérie, tous les événements ont été annulés ou reportés. La priorité absolue de l'ANPT étant la santé et la sécurité de ses employés et de leur famille, nous vous prions de suivre les consignes du ministère de la santé et de l'OMS.

Reference	ANPT-2020-BV-03
Titre	Bulletin de veille N° 3
Date de version	31 mars 2020
Contact	ssi@anpt.dz