BULLETIN DE VEILLE N°1

ANPT-2020-BV-01

« Les gagnants seront ceux qui restructurent la manière dont l'information circule dans leur entreprise..» ***- Bill Gates-***

Janvier 2020

Alertes de sécurité

Réseaux sociaux

TikTok corrige des failles de sécurité

08 janvier 2020

Découvertes par des chercheurs de CheckPoint, les failles de sécurité de l'application de partage de vidéos et de réseaux sociaux TikTok auraient pu mettre en danger la vie privée de ses utilisateurs. La première vulnérabilité que les chercheurs ont découvert a été dans la fonctionnalité SMS de l'application TikTok. Pour aider les utilisateurs à installer l'application, le site Web leur permet de s'envoyer un SMS avec un lien de téléchargement. Il a été constaté qu'un attaquant peut l'exploiter en modifiant le paramètre URL de téléchargement. L'attaquant peut envoyer un message SMS usurpé contenant un lien malveillant appartenant à l'attaquant. Cependant, ce n'est pas la seule vulnérabilité que les chercheurs ont découvert. Le sous-domaine TikTok Ads du site Web officiel de TikTok était vulnérable aux attaques Cross-Site Scripting (XSS), permettant aux attaquants de supprimer des vidéos, rendre publiques des vidéos privées ou publier leurs propres vidéos. En combinant les deux vulnérabilités il est possible de récupérer des informations sensibles non destinées à la consommation publique, y compris les noms, les adresses e-mail et la date de naissance des utilisateurs. Les problèmes signalés sont corrigés dans la dernière version de l'application.

Source : *https://zd.net/39RyE8h*

Microsoft

Microsoft corrige une faille critique «NSACrypt» signalée par la NSA

15 janvier 2020

Microsoft a publié des correctifs de sécurité pour 49 vulnérabilités dans le cadre du correctif du 14 janvier 2020. Sur ces vulnérabilités, 7 ont été jugées « critiques ». C'est l'une des vulnérabilités les plus notables et la première signalée pour la National Security Agency (NSA).

La faille surnommée «NSACrypt» ou «Windows CryptoAPI « Spoofing», toucherait des millions d'ordinateurs Windows 10. La vulnérabilité réside dans le module Crypt32.dll qui contient diverses fonctions de cryptographie ECC (Elliptic Curve Cryptography) et de certificat. Un attaquant peut exploiter la faille pour usurper des logiciels légitimes, ce qui pourrait faciliter l'exécution de code malveillants sur un ordinateur vulnérable. «Cela peut permettre diverses actions, y compris, mais sans s'y limiter, l'interception et la modification des communications cryptées TLS ou l'usurpation d'une signature Authenticode ».

La NSA et Microsoft affirment que la vulnérabilité n'a pas encore été exploitée. Cependant, en raison de la classification de la vulnérabilité, Microsoft a publié des correctifs dans la dernière édition du Patch Tuesday. Les détails techniques de la faille ne sont pas encore accessibles au public.

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

Détails CVE : *http://bit.ly/2R55gUK*

Une vulnérabilité zero-day dans Internet Explorer

19 janvier 2020

Une nouvelle vulnérabilité découverte dans Internet Explorer est exploitée sur le net. Cette vulnérabilité référencée CVE-2020-0674 pourrait corrompre la mémoire de telle manière qu'un attaquant pourrait exécuter du code arbitraire dans le contexte de l'utilisateur actuel. Si l'utilisateur actuel est connecté avec des droits administrateur, un attaquant pourrait alors installer des programmes ; afficher, modifier ou supprimer des données ; ou créer de nouveaux comptes avec des droits d'utilisateur complets. Dans un scénario d'attaque basé sur le Web, un attaquant pourrait héberger un site Web spécialement conçu pour exploiter la vulnérabilité via Internet Explorer, puis convaincre un utilisateur de consulter le site Web, par exemple, en envoyant un e-mail.

Les versions affectées : Internet Explorer 9, 10 et 11 sur Windows 7, 8.1, RT 8.1, 10, Server 2008, 2008 R2, Server 2012, Server 2016 et Server 2019.

Aucune solution pratique n'est disponible pour ce problème. Selon l'avis de Microsoft, empêcher le chargement de la bibliothèque JScript.dll peut bloquer manuellement l'exploitation de cette vulnérabilité. Veuillez consulter l'avis pour plus de détails sur les mesures de contournement.

Source *: http://bit.ly/2v75O44*

Android

La mise à jour d'Android corrige 40 vulnérabilités

07 janvier 2020

Google a publié le bulletin de sécurité Android pour janvier 2020, avec des correctifs pour 40 vulnérabilités. Le bulletin de sécurité Android de janvier 2020 a été divisé en deux parties : la première corrige 7 vulnérabilités dans le Framework, Media Framework et System, tandis que la seconde comprend des correctifs pour 33 failles de sécurité dans Kernel, Qualcomm. Le plus grave de ces problèmes est une vulnérabilité de sécurité critique référencée CVE-2020-0002 dans le cadre Media qui pourrait permettre à un attaquant distant utilisant un fichier spécialement conçu d'exécuter du code arbitraire dans le contexte d'un processus privilégié. Une autre vulnérabilité importante est une faille critique dans le pilote Realtek rtlwifi, qui pourrait entraîner l'exécution de code à distance.

Google a également publié un bulletin de sécurité distinct détaillant les vulnérabilités corrigées dans les appareils Pixel.

Systèmes affectés : Android 8.0, 8.1, 9 et 10.

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

Oracle

Des correctifs critiques d'Oracle pour janvier 2020

15 janvier 2020

Oracle a publié sa mise à jour des correctifs critiques pour janvier 2020 en incluant 334 correctifs de vulnérabilité sur plusieurs produits.

12 vulnérabilités dans Oracle Database Server ont été corrigées. Les attaquants peuvent exploiter à distance trois de ces vulnérabilités sans les informations d'identification de l'utilisateur. L'une des vulnérabilités de gravité élevée est la vulnérabilité CVE-2020-2510 qui affecte Core RDMS.

Un autre bug de gravité élevée CVE-2019-10072 affecte Workload Manager (Apache Tomcat).

De plus, Oracle a corrigé 19 nouvelles failles de sécurité dans MySQL. Six d'entre elles peuvent être exploitées à distance sans informations d'identification utilisateur.

12 nouvelles vulnérabilités de sécurité ont été détectées dans Oracle Java SE. Toutes ces vulnérabilités peuvent également être exploitées à distance sans informations d'identification utilisateur. Une vulnérabilité référencée CVE-2020-2604 de gravité élevée avec un impact sur le composant de sérialisation de Java SE a été détectée.

Dans certains cas, les acteurs malveillants ont réussi à exploiter les vulnérabilités parce que les organisations n'ont pas appliqué les correctifs Oracle nécessaires. Oracle recommande fortement "que les clients restent sur les versions activement prises en charge et appliquent les correctifs de mise à jour des correctifs sans délai", comme indiqué dans le dernier avis de sécurité.

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

Cisco

Un bug dans Cisco Webex de type RCE

08 janvier 2020

Une vulnérabilité dans l'interface de gestion Web de Cisco Webex Video Mesh pourrait permettre à un attaquant distant authentifié d'exécuter des commandes arbitraires sur le système affecté.

La vulnérabilité référencée CVE-2019-1600 est due à une validation incorrecte des entrées fournies par l'utilisateur par l'interface de gestion Web du logiciel concerné. Un attaquant pourrait exploiter cette vulnérabilité en se connectant à l'interface de gestion Web avec des privilèges administratifs et en fournissant des demandes spécialement conçues à l'application. Un exploit réussi pourrait permettre à l'attaquant d'exécuter des commandes arbitraires sur le système d'exploitation Linux sous-jacent avec les privilèges root sur un nœud cible.

Version affectées: Les versions du logiciel Cisco Webex Video Mesh antérieures à 2019.09.19.1956m.

Cisco a publié des mises à jour qui corrigent cette vulnérabilité. Il n'existe aucune solution de contournement qui résout cette vulnérabilité.

Source *: http://bit.ly/2NXHk3Z*

Une vulnérabilité CSRF dans l'interface Web des logiciels Cisco IOS et Cisco IOS XE

08 janvier 2020

Une vulnérabilité dans l'interface Web de Cisco IOS et du logiciel Cisco IOS XE pourrait permettre à un attaquant distant non authentifié de mener une attaque de type CSRF sur un système affecté.

La vulnérabilité est due à l'insuffisance des protections CSRF pour l'interface utilisateur Web sur un appareil affecté. Un attaquant pourrait exploiter cette vulnérabilité en persuadant un utilisateur de l'interface de suivre un lien malveillant. Un exploit réussi pourrait permettre à l'attaquant d'effectuer des actions arbitraires avec le niveau de privilège de l'utilisateur ciblé. Si l'utilisateur dispose de privilèges administratifs, l'attaquant pourrait modifier la configuration, exécuter des commandes ou recharger un appareil affecté.

Versions affectées : Les périphériques Cisco qui exécutent une version vulnérable du logiciel Cisco IOS ou Cisco IOS XE antérieure à 16.1.1 avec la fonctionnalité HTTP Server activée.

Cisco a publié des mises à jour logicielles qui corrigent cette vulnérabilité. Il n'existe aucune solution de contournement qui résout cette vulnérabilité.

Source *: http://bit.ly/2RchQ4J*

Intel

La nouvelle attaque «CacheOut» cible les CPU Intel

27 janvier 2020

Une vulnérabilité référencée CVE-2020-0549 comme dans la plupart des processeurs Intel qui permet à un attaquant de cibler des données plus spécifiques, même stockées dans l'enclave SGX sécurisée d'Intel.

Parmi les menaces que CacheOut fait peser sur les fournisseurs de cloud est la fuite de données provenant d'hyperviseurs (moniteurs de machine virtuelle) et des machines virtuelles qui s'exécutent sur eux. Intel a déclaré qu'il prévoyait de publier des mesures d'atténuation pour résoudre le problème dans un proche avenir. Ceux-ci sont normalement envoyés aux utilisateurs sous forme de mises à jour du BIOS ou des pilotes. Pratiquement tous les processeurs Intel sont potentiellement affectés par CacheOut, à l'exception des processeurs sortis après le quatrième trimestre de 2019. Les processeurs AMD ne sont pas affectés, selon les détails publiés sur un site CacheOut dédié. Les processeurs fabriqués par IBM et ARM peuvent être affectés, mais n'ont pas été confirmés.

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

Actualités

Les pirates informatiques exploitent la vulnérabilité d'Android pour installer des logiciels malveillants

06 janvier 2020

Des chercheurs en sécurité de Trend Micro ont observé trois applications malveillantes sur Google Play qui visent à compromettre les appareils des victimes et à voler des informations.

Les trois applications incluant «**Camero, FileCryptManager et CallCam**» fonctionnent ensemble pour compromettre l'appareil d'une victime et collecter des informations sur les utilisateurs. Parmi les trois Camero est celle qui exploite la vulnérabilité d'utilisation après libération CVE-2019-2215.

Il s'agit de la première attaque repérée à l'état sauvage à l'aide d'exploits CVE-2019-2215 résidant dans Binder. En exploitant cette vulnérabilité, les attaquants peuvent télécharger des fichiers sans interaction de l'utilisateur. […]

Pour échapper à la détection, ils utilisent de nombreuses techniques telles que l'obscurcissement, le chiffrement des données et l'appel de code dynamique. Les trois applications se sont révélées actives depuis mars 2019. Les applications ont depuis été supprimées de Google Play.

Source : http://bit.ly/2ZVusQz

Le gouvernement américain confirme un avertissement de sécurité critique pour les utilisateurs de Firefox

09 janvier 2020

L'Agence de cyber sécurité et de sécurité des infrastructures (CISA) des États-Unis a publié une notification qui "encourage" les utilisateurs et les administrateurs à mettre à jour le navigateur Web Mozilla Firefox. Ceci, bien que Firefox ait publié une mise à jour importante du programme, vers la version 72, le 7 janvier.

La mise à jour a inclus un patch pour la vulnérabilité zero-day activement exploitée, qui peut permettre à un acteur malveillant de prendre le contrôle des ordinateurs des utilisateurs.

Vous pouvez vérifier si Firefox est sûr en cliquant sur le menu en haut à droite du navigateur et en sélectionnant "À propos de Firefox" dans la section Aide.

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

Plus de 200 millions de modems filaires vulnérables à une nouvelle attaque dangereuse

10 janvier 2020

Un groupe de chercheurs en sécurité a découvert une faille qui met en danger un nombre ahurissant d'utilisateurs de modems filaires. Un pirate qui parvient à compromettre un modem en utilisant le repérage par câble obtient un contrôle total sur le trafic entrant et sortant. Étant donné qu'un modem se trouve devant le routeur, chaque périphérique du réseau est mis en danger.

L'attaquant peut espionner l'activité de navigation, réacheminer le trafic vers des domaines malveillants ou même zombifier des appareils pour les utiliser dans des attaques de botnet. Étant donné que le modem lui-même a été compromis, un attaquant qualifié pourrait se cacher dans l'ombre sans être détecté une fois qu'il ou elle a pris le contrôle […].

Chose choquante, quatre des dix modèles vulnérables identifiés n'avaient besoin d'aucune autorisation pour accéder à l'analyseur. Deux autres ont utilisé la combinaison indéniablement horrible du spectre comme nom d'utilisateur et mot de passe, mais à condition qu'un attaquant potentiel doive avoir accès à un appareil connecté au réseau privé desservi par le modem filaire. C'est une barre beaucoup plus élevée, une vulnérabilité qui peut être exploitée sur Internet. Cependant, obtenir ce type d'accès n'est pas si difficile. Tout ce qu'il faut, c'est un e-mail de phishing convaincant ou un téléchargement en voiture, et étant donné le type de contrôle que Cable Haunt donnerait à un attaquant, il y a beaucoup de motivation pour tenter de le faire.

Source : *http://bit.ly/382jfk2*

Le cheval de Troie Android tue Google Play Protect et crache de fausses critiques d'application

11 janvier 2020

Une souche de malware Android camouflée en tant qu'application système est utilisée par des internautes malveillants. Le malware lourdement obscurci surnommé **TrojanDropper.-AndroidOS.Shopper.a** utilise une icône système et le nom ConfigAPKs qui ressemble étroitement au nom d'un service Android légitime responsable de la configuration de l'application la première fois qu'un appareil est démarré.

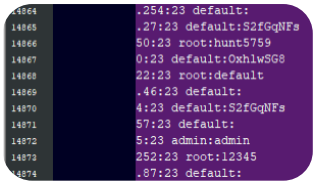
Les attaquants utilisent Shopper.a pour augmenter les notes d'autres applications malveillantes sur le Play Store, publient de fausses critiques sur les entrées des applications, installent d'autres applications du Play Store ou des magasins d'applications tiers etc. De plus, le cheval de Troie peut afficher des messages publicitaires sur le périphérique infecté, créer des raccourcis vers les sites publicitaires et effectuer d'autres actions." Cela se fait en abusant du service d'accessibilité, une tactique connue utilisée par les logiciels malveillants Android pour effectuer un large éventail d'activités malveillantes sans nécessiter d'interaction avec l'utilisateur.

Google a révélé que Play Protect a détecté et supprimé environ 1700 applications infectées par **le malware Joker** Android (également connu sous le nom de **Bread**) du Play Store depuis que la société a commencé à suivre cette souche au début de 2017.

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

Hacker fuit plus de 500 000 informations d'identification Telnet pour les appareils IoT

19 janvier 2020



Un pirate a publié cette semaine une énorme liste d'informations d'identification Telnet pour plus de 515 000 serveurs, routeurs domestiques et appareils «intelligents» IoT (Internet of Things).

La liste, qui a été publiée sur un forum de piratage populaire, comprend l'adresse IP de chaque appareil, ainsi qu'un nom d'utilisateur et un mot de passe pour le service Telnet.

La liste a été compilée en recherchant sur Internet l'ensemble des appareils qui exposaient leur port Telnet. Le pirate a essayé d'utiliser (1) les noms d'utilisateurs et mots de passe par défaut définis en usine, ou (2) des combinaisons de mots de passe personnalisées mais faciles à deviner.

La liste compilée par le pirate est connue sous le nom de «liste de robots», sur laquelle les opérations de botnet IoT s'appuient pour se connecter aux appareils et installer les logiciels malveillants afin de réaliser des attaques de type DDoS. […]Un expert en sécurité IoT a déclaré que même si certaines entrées de la liste ne sont plus valides parce que les appareils peuvent avoir changé leurs adresses IP ou leurs mots de passe, les listes restent incroyablement utiles pour un attaquant qualifié.

En effet, non seulement les utilisateurs d'appareils et les maisons intelligentes sont à risque, mais l'entreprise est également confrontée à de nouveaux défis de sécurité en raison de ces appareils IoT non sécurisés, a déclaré Raphael Reich, vice-président du marketing de la société de sécuritéb CyCognito.

Source *: https://zd.net/36dHfz5*

Le ransomware Ako pourrait être la prochaine menace pour votre réseau

13 janvier 2020

Le ransomware Ako a été découvert après qu'une victime en ait fait part sur un forum. Bleeping Computer a analysé le malware et a découvert qu'il s'agissait d'un nouveau ransomware.

Selon la victime, le ransomware a affecté le bureau Windows 10 et le serveur Windows SBS 2011.

Ako travaille d'une manière assez sophistiquée. En entrant dans le système, le ransomware supprime d'abord les clichés instantanés de volume et les sauvegardes récentes. Il désactive ensuite l'environnement de récupération Windows avant de commencer le chiffrement des données.

Lors du cryptage des fichiers, il ajoute aux fichiers une extension générée aléatoirement. Il ajoute également un marqueur de fichier CECAEFBE aux fichiers cryptés afin que le ransomware puisse les identifier.

Pendant le chiffrement, il ignore les fichiers avec les extensions .exe, .sys, .dll, .ini, .key, .lnk et .rdp. Il exclut également les chemins de fichiers manquant $, AppData, Program Files, Program Files (x86), AppData, boot, PerfLogs, Tor Browser, Windows strings, ProgramData, Google, Intel, Microsoft, Application Data.

Il vérifie ensuite les autres machines connectées sur le réseau pour terminer le processus de cryptage. Au final, le ransomware place la note de rançon intitulée «ako-readme.txt» sur le bureau.

À l'heure actuelle, la technique utilisée par les attaquants pour distribuer le logiciel malveillant n'était pas claire. Cependant, selon des chercheurs, il est probable que les attaquants exploitent les services Remote Desktop pour propager l'infection.

Source *: http://bit.ly/35PxgZT*

FTCODE Ransomware vole maintenant les informations d'identification de Chrome et Firefox

21 janvier 2020

FTCODE, un ransomware basé sur PowerShell qui cible les utilisateurs de langue italienne, des nouvelles fonctionnalités dans FTCODE ont été ajoutées,

notamment la possibilité de balayer le navigateur Web enregistré et les informations d'identification du client de messagerie des victimes. Les chercheurs affirment que de nouvelles versions du ransomware visent désormais à voler les informations d'identification d'Internet Explorer et de Mozilla Firefox, ainsi que des clients de messagerie Mozilla Thunderbird, Google Chrome et Microsoft Outlook […]."Cette tendance vers des moyens plus créatifs d'exploiter ... est une raison impérieuse de se concentrer sur des mesures préventives plus fortes et pas seulement sur la capacité de restaurer rapidement les fichiers après que l'infection se soit produite", a déclaré Erich Kron, défenseur de la sensibilisation à la sécurité chez KnowBe4, dans un courriel.

Source : http://bit.ly/30QrJIE

Détails Technique : http://bit.ly/2ulDPNB

Un bug Facebook a révélé des administrateurs anonymes de pages

10 janvier 2020

Une mauvaise mise à jour du code a permis à quiconque de révéler facilement les comptes publiés sur les pages Facebook - y compris les célébrités et les politiciens - pendant plusieurs heures.

Les comptes derrières ces pages sont anonymes, sauf si un propriétaire de page décide de rendre les administrateurs publics. Mais un bug qui était en direct du jeudi soir au vendredi matin a permis à quiconque de révéler facilement les comptes exécutant une page.

Facebook a rapidement proposé un correctif pour celui-ci. Malgré le correctif des captures d'écran ont circulé sur 4chan, Imgur et les réseaux sociaux semblant montrer les comptes derrière les pages. Pour exploiter le bug, il suffisait d'ouvrir une page cible et de vérifier l'historique des modifications d'un article. Facebook a affiché par erreur le ou les comptes qui ont apporté des modifications à chaque publication, plutôt que seulement les modifications elles-mêmes.

Source : http://bit.ly/2NlnDCJ

Les téléphones émis par le gouvernement américain exécutent un «malware chinois»

09 janvier 2020

Les téléphones mobiles offerts aux familles à faible revenu via un programme du gouvernement américain sont préinstallés avec des logiciels malveillants chinois, selon une société de sécurité.

Malwarebytes a déclaré avoir reçu plusieurs plaintes selon lesquelles des applications préinstallées sur le téléphone étaient malveillantes Le téléphone basé sur Android - UMX U686CL - est fabriqué par une société chinoise.

Et il semble que ce soit une variante d'**Adups**, un malware précédemment tracé en Chine, qui transmet le texte, l'emplacement des appels et les données d'application à un serveur chinois toutes les 72 heures.

En 2016, le chercheur Ryan Johnson, de la société de sécurité Kryptowire, a découvert que plus de 700 millions de smartphones Android, dont certains aux États-Unis, avaient installé **Adups**. Son rapport a incité Google à enquêter et le Department of Homeland Security.

Le programme est géré par la Federal Communications Commission, qui n'a pas répondu aux demandes de commentaires de BBC News.

Source : https://bbc.in/2uJvjbv

Evènements

Evènements du mois

HackINI (Hack initiation), ALGER

25 janvier 2020

http://bit.ly/2vtaVvC

HackINI est un évènement organisé chaque année par le club Shellmates de l'école nationale supérieur d'informatique. Dans sa huitième édition en partenariat avec Deloitte, des ateliers, des conférences et des concours CTF ont été organisés. Les thèmes des ateliers sont : les autorisations des fichiers Linux, et SELinux, les tests de pénétration, Exploitation de serveur web, introduction sur docker et Elastic Stack.

Forum International de la Cybersécurité (FIC), Lille

28-30 janvier 2020

http://bit.ly/2GvpFw9

Le Forum International de la Cybersécurité (FIC) a regroupé des personnalités emblématiques de la cybersécurité en Europe, pour accompagner le développement européen et international du FIC. Des panels, des conférences et des ateliers ont eu lieu, aussi un FORUM favorisant la réflexion et l'échange au sein de l'écosystème européen de la cybersécurité et un SALON dédié aux rencontres entre acheteurs et fournisseurs de solutions de cyber sécurité.

Reference	ANPT-2020-BV-01
Titre	Bulletin de veille N°1
Date de version	30 janvier 2020
Contact	ssi@anpt.dz