BULLETIN DE VEILLE N°2

ANPT-2019-BV-02

« La prochaine vague de cyberattaques ne consistera pas à détruire des données mais à les modifier. » - James Clapper-

Juin 2019

Alertes de sécurité

Réseaux sociaux

Une vulnérabilité dans Viber Desktop (Windows)

03 juin 2019

Une vulnérabilité classée critique et référencée CVE-2019-12569 a été trouvée dans Viber Desktop version 10.6.x sous Windows. Elle permettrait de perpétuer une attaque à distance et cela sans aucune forme d'authentification. Les détails techniques de l'exploitation possible de cette vulnérabilité ne sont pas publiés à ce jour.

Il est recommandé de mettre à jour l'application à la version 10.7.x.

Source *: https://vuldb.com/fr/?id.135844*

Détails CVE *: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12569*

Vulnérabilité dans WhatsApp

24 juin 2019

Une vulnérabilité a été découverte début mai dans l'application mobile WhatsApp. Cette vulnérabilité permettait d'exécuter du code malveillant à distance sur plus d'1,5 milliards de téléphone, elle aurait été exploitée par une société éditant le logiciel de surveillance mobile Pegasus.

Cette vulnérabilité a finalement été corrigée par WhatsApp le 22/06/2019. Il est recommandé de mettre à jour l'application WhatsApp depuis les App stores officiels.

Source *: https://www.mag-securs.com/communiques/id/47153/vulnerabilite-dans-whatsapp-que-risquez-vous.aspx*

Microsoft

Multiples vulnérabilités corrigées dans les produits Microsoft

12 juin 2019

Un bulletin de mises à jour de sécurité a été publié par Microsoft corrigeant plusieurs vulnérabilités sur ses produits.

Il est recommandé d'appliquer cette mise à jour dans les meilleurs délais.

Produits affectés: Adobe Flash Player, Microsoft Windows, Internet Explorer, Microsoft Edge, Microsoft Office and Microsoft Office Services and Web Apps, ChakraCore, Skype for Business and Microsoft Lync, Microsoft Exchange Server, Azure, Microsoft Outlook for Android.

Source *: https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/253dc509-9a5b-e911-a98e-000d3a33c573*

Adobe Flash Player

Vulnérabilité dans Adobe Flash Player (AFP)

11 juin 2019

Une vulnérabilité référencée CVE-2019-7845 a été découverte dans Adobe Flash Player. Elle permet à un attaquant de provoquer une exécution de code arbitraire.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

Systèmes affectés : les versions antérieures à 32.0.0.207 d'AFP Desktop Runtime et AFP pour Chrome sur Windows, macOS et Linux. AFP pour Ms Edge et IE 11 sur Windows 10 et 8.1

Détails CVE *:http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7845*

Source *: https://helpx.adobe.com/security/products/flash-player/apsb19-30.html*

VMware

Multiples vulnérabilités dans VMware Tools et Workstation

06 juin 2019

De multiples vulnérabilités ont été découvertes dans VMware Tools et Workstation. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service et une atteinte à la confidentialité des données.

Ces vulnérabilités correspondent au CVE suivants : CVE-2019-5522, CVE-2019-5525

Systèmes affectés : VMware Tools versions 10.x antérieures à 10.3.10 sur Windows, VMware Workstation versions 15.x antérieures à 15.1.• sur Linux.

Bulletin : *https://www.vmware.com/security/advisories/VMSA-2019-0009.html*

Source : https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-253/

Google

Vulnérabilité dans Google Chrome

14 juin 2019

Une vulnérabilité référencée CVE-2019-5842 a été découverte dans Google Chrome. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs.

Système affecté : Google Chrome versions antérieures à 75.0.3770.90 sur Windows, Mac et Linux.

Source : *https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-desktop_13.html*

Détails CVE : *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5842*

Multiples vulnérabilités dans Google Android

03 juin 2019

De multiples vulnérabilités ont été découvertes dans Google Android. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges.

Se référer au bulletin de sécurité de l'éditeur pour les détails des CVEs, ainsi pour l'obtention des correctifs.

Systèmes affectés : Google Android toutes versions n'intégrant pas le correctif de sécurité du 3 juin 2019.

Source : *https://source.android.com/security/bulletin/2019-06-01.html*

PhpMyAdmin

Vulnérabilité dans phpMyAdmin

04 juin 2019

Une vulnérabilité a été découverte dans phpMyAdmin. Elle permet à un attaquant de provoquer une injection de requêtes illégitimes par rebond (CSRF).

La solution est de mettre à niveau à la version 4.9.0 ou une version plus récente.

Versions affectées : phpMyAdmin toutes versions antérieures à 4.9.0

Détails CVE : *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12616*

Source : *https://www.phpmyadmin.net/security/PMASA-2019-4/*

Mozilla

Multiples vulnérabilités dans Mozilla Thunderbird

14 juin 2019

De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance.

Ces vulnérabilités correspondent aux CVE suivants : CVE-2019-11703, CVE-2019-11704, CVE-2019-11705, CVE-2019-11706.

Selon le bulletin de sécurité de l'éditeur, il est recommandé de mettre à jour Thunderbird à la version 60.7.1.

Source : *https://www.mozilla.org/en-US/security/advisories/mfsa2019-17/*

Apache

Une vulnérabilité dans Apache Tomcat mène à un déni de service

21 juin 2019

Une vulnérabilité, référencée CVE-2019-10072 et classée problématique, a été découverte dans Apache Tomcat v. 8.5.40/9.0.19 (Application Server Software). La manipulation de valeurs d'entrées aléatoire provoque un déni de service du serveur. L'exploitation ne nécessite aucune forme d'authentification. Les détails techniques de l'exploitation ne sont pas publiés à ce jour.

Aucune information de contremesures et de correctifs n'est disponible. Il est suggéré de surveiller attentivement l'application ou de la remplacer par un produit alternatif.

Source : *https://vuldb.com/fr/?id.136822*

Détails CVE : *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10072*

Sophos

Multiples vulnérabilités dans Sophos XG firewall (Admin portal)

20 juin 2019

De multiples vulnérabilités classées critiques ont été découvertes dans le pare-feu Sophos XG. La manipulation des paramètres dans Admin portal (dbname et username) permet de mener des attaques de classe élévation de privilèges et injection SQL.

L'attaque peut être initialisée à distance. Les détails techniques sont connus (POC : Proof of Concept), mais aucun exploit n'est disponible.

Aucune information n'est disponible concernant de possibles contremesures. Il est suggéré de surveiller de très près le produit vulnérable.

Source : *https://vuldb.com/?recent.20190620*

Détails CVEs : *CVE-2018-16118, CVE-2018-16117, CVE-2018-16116*

Pfsense

Une vulnérabilité XSS dans le pare-feu applicatif Pfsense 2.4.4

25 juin 2019

La vulnérabilité CVE-2019-12949 permet de mener une attaque à distance. Une seule session d'authentification est nécessaire pour l'exploitation. Les détails techniques sont connus, mais aucun exploite n'est disponible.

Aucun correctif n'est encore publié par l'éditeur. Il est recommandé de suivre et de renforcer les sessions d'authentification au produit.

Source : *https://vuldb.com/fr/?id.136865*

Détails CVE : *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12949*

Actualité

Ransomware : cette ville de Floride paie 600 000 $ pour récupérer ses données

20 juin 2019

Le conseil municipal de Riviera Beach, en Floride, a voté cette semaine la décision de payer plus de 600 000 $ à un gang utilisant un ransomware afin que les fonctionnaires municipaux puissent récupérer les données qui ont été verrouillées et chiffrées il y a plus de trois semaines.

La décision de la ville, rapportée par CBS News, a été prise après que les fonctionnaires aient conclu qu'il n'y avait aucun autre moyen de récupérer les dossiers de la ville […].

L'accès aux données de Riviera City est verrouillé depuis le 29 mai dernier, lorsqu'un employé du service de police de Riviera Beach a **ouvert un courriel** et installé un ransomware sur le réseau de la ville.

Le logiciel malveillant a verrouillé les fichiers et fermé tous les services numériques de la ville. Seul les services de secours ont pu continuer à fonctionner, quoique de façon limitée […].

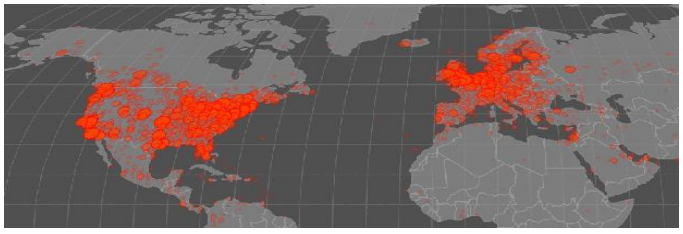
Au début, la ville n'avait pas l'intention de payer les criminels, mais il est devenu évident au cours des dernières semaines qu'elles ne seraient pas en mesure de retrouver l'accès à toutes leurs données, qui n'avaient pas été correctement sauvegardées […].
Cependant, Riviera City ne sera pas la victime qui a payé la plus grosse demande de rançon. Cet "honneur" va à la société sud-coréenne d'hébergement web Internet Nayana, qui a payé 1,3 milliard de won (1,14 million de dollars) en bitcoins à un hacker suite à une attaque en juin 2017.

Source : *https://www.zdnet.fr/actualites/ransomware-cette-ville-de-floride-paie-600-000-pour-recuperer-ses-donnees-39886265.htm#xtor=123456*

Le nouveau malware d'Echobot est un concentré de vulnérabilités

18 juin 2019

Des chercheurs en sécurité ont repéré une nouvelle variante de Mirai. Le programme malveillant Echobot cible un large éventail de périphériques IoT et d'applications d'entreprise.



[…] Il ne se passe pas un mois sans qu'un nouveau botnet majeur ne surgisse de nulle part et ne lance des attaques massives contre des terminaux - soit en utilisant des **identifiants par défaut** pour prendre le contrôle du périphérique, soit en utilisant des exploits pour d'anciennes failles de sécurité que les propriétaires n'ont pas corrigées.

Nouvelle variante Mirai nommée Echobot

Le dernier-né de cette longue lignée de fléaux Mirai est une nouvelle variante appelée Echobot. Créé à la mi-mai, le malware a d'abord été décrit par Palo Alto Networks dans un rapport publié début juin, puis dans un autre rapport paru la semaine dernière par des chercheurs en sécurité d'Akamai […].
Lorsque les chercheurs de Palo Alto Networks l'ont repéré pour la première fois début juin, Echobot utilisait des exploits pour 18 vulnérabilités. Dans le rapport d'Akamai, une semaine plus tard, Echobot en exploitait 26 […] ils commencent par choisir des exploits au hasard, mais ils ne conservent que ceux qui apportent un grand nombre de terminaux infectés (bots) et ne rejettent que ceux qui ne fonctionnent pas. […] l'arsenal actuel d'exploits d'Echobot peut être considéré comme une liste des vulnérabilités qui produisent le plus de bots.

Source : *https://www.zdnet.fr/actualites/le-nouveau-malware-d-echobot-est-un-concentre-de-vulnerabilites-39886143.htm#xtor=123456*

Un nouvel outil de piratage iranien fuite sur Telegram

04 juin 2019

Le nouvel outil de piratage iranien au nom de Jason a été publié aujourd'hui en ligne, dans un canal de Telegram. Il est destiné à brute forcé les serveurs de messagerie Microsoft Exchange à l'aide de listes précompilées de combinaisons de noms d'utilisateur et de mots de passe.

La source de cette fuite, surnommé Lab Dookhtegan, est la même qui, en avril, a divulgué le code source de six autres outils de piratage iraniens, ainsi que d'autres informations sensibles sur les victimes du piratage et les membres du piratage du gouvernement iranien.

Omri Segev Moyal, chercheur en sécurité a déclaré que l'outil avait été compilé en 2015, ce qui signifie que son utilisation date depuis au moins quatre ans. […]

Source : *https://www.zdnet.fr/actualites/un-nouvel-outil-de-piratage-iranien-fuite-sur-telegram-39885479.htm#xtor=123456*

Seulement 5,5% de toutes les vulnérabilités sont exploitées

05 juin 2019

Une nouvelle étude publiée cette semaine éclaire un peu plus l'univers de l'exploitation des vulnérabilités, révélant combien de failles de sécurité découvertes au cours des dix dernières années ont été réellement exploitées.
L'étude - considérée comme la plus vaste du genre à ce jour - révèle que seulement 4183 failles de sécurité sur un total de 76000 vulnérabilités découvertes entre 2009 et 2018 ont été exploitées dans des attaques.

Plus intéressant encore, les chercheurs ont constaté qu'il n'y avait aucune corrélation entre la publication d'un code d'exploitation sous forme d'un PoC sur les sites xeb publics et le début des tentatives d'exploitation.

L'équipe de recherche note que sur les 4183 failles de sécurité exploitées entre 2009 et 2018, seulement la moitié étaient associées à un code d'exploitation répertorié sur les sites publics.

Cela signifie que l'absence d'un PoC public n'a pas nécessairement empêché les attaquants d'exploiter certaines vulnérabilités - certains pirates informatiques réalisant leurs propres exploits au besoin.

Les failles sévères ont été les plus exploitées

En outre, l'étude constate que la plupart des vulnérabilités exploitées dans la nature sont des failles de sécurité dont le score de gravité CVSSv2 est élevé (qui peut aller de 1 à 10, le 10 étant attribué aux vulnérabilités les plus dangereuses et les plus faciles à exploiter) […].

Des détails supplémentaires sur cette étude peuvent être trouvés dans un livre blanc intitulé *"Improving Vulnerability RemediationThrough Better Exploit Prediction*" présenté lors du Workshop sur l'économie de la sécurité de l'information à Boston.

Source : *https://www.zdnet.fr/actualites/seulement-55-de-toutes-les-vulnerabilites-sont-exploitees-39885533.htm#xtor=123456*
L'étude : *https://weis2019.econinfosec.org/wpcontent/uploads/sites/6/2019/05/WEIS_2019_paper_53.pdf*

RGPD : 400 000€ d'amende pour une agence immobilière

Sergic est une société spécialisée dans la promotion et la gestion immobilière, l'achat, la vente, et la location de biens immobiliers. Elle édite par ailleurs le site web www.sergic.com. Une interface stratégique qui permet aux personnes intéressées de candidater et donc de déposer des pièces justificatives pour constituer des dossiers. Problème, en août 2018, un utilisateur mécontent du site signale avoir pu accéder depuis son espace personnel sur le site, à des documents enregistrés par d'autres utilisateurs […]. La Cnil a considéré que la société avait *manqué à son obligation de préserver la sécurité des données personnelles des utilisateurs* de son site, prévue par l'article 32 du ***règlement général sur la protection des données*** (RGPD). De fait, la société n'avait pas mis en place de procédure d'authentification des utilisateurs du site permettant de s'assurer que les personnes accédant aux documents étaient bien celles à l'origine de leur téléchargement […].

Source : *https://www.zdnet.fr/actualites/rgpd-400-000-d-amende-pour-une-agence-immobiliere-39885717.htm*

La NASA piratée via un ordinateur Raspberry Pi non autorisé connecté à ses serveurs

24 juin 2019

La NASA a confirmé que les pirates informatiques avaient eu accès au Jet Propulsion Laboratory (JPL) l'année dernière et qu'ils étaient capables de voler 500 Mo de données relatives aux missions sur Mars. Les pirates ont pénétré dans le réseau de la NASA en avril 2018 et l'intrusion n'a pas été détectée pendant près d'un an.

Selon le rapport du BIG, un ordinateur Raspberry Pi non autorisé connecté aux serveurs JPL sans audit de sécurité permet aux pirates d'accéder au réseau, ce qui leur a permis de pénétrer plus avant dans le réseau […].

"Le cyber attaquant de l'incident d'avril 2018 a exploité le manque de segmentation du réseau JPL pour se déplacer entre différents systèmes connectés à la passerelle, y compris plusieurs opérations de mission JPL et le DSN."

En outre, le rapport indique que les administrateurs système n'ont pas examiné les journaux du système et des applications en raison d'une mauvaise compréhension des responsabilités en place, ce qui a permis aux attaquants de rester non détectés pendant près d'un an […].

«Le NIST recommande aux entreprises de procéder à des examens périodiques des processus et des procédures pour assurer une gestion efficace des journaux afin de détecter les menaces dans leur environnement informatique.»

Source : *https://gbhackers.com/nasa-hacked-raspberry-pi/*

Evènements

Evènements du mois

L'AFRICAN CYBER SECURITY SUMMIT

10-11 juin 2019, Alger.

https://acss.forum-sit.dz/

Le sommet africain de cyber sécurité a réuni des décideurs IT (DSI & RSSI) d'entreprises algériennes et africaines, ainsi que des éditeurs mondiaux de solutions de cyber sécurité.

L'évènement s'est déroulé pendant deux jours au Centre International des Conférences (CIC). Des conférences, des tables rondes et des ateliers ont été organisés pour échanger et discuter sur les défis et les priorités en termes de sécurité exigés par les nouvelles technologies. Les thématiques ont été focalisées sur l'importance de la mise en place de mécanismes pour la protection des données, principalement celles à caractère personnel ainsi que les dispositions de la loi algérienne 18-07 du 10 Juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.

Les vidéos relatives aux conférences plénières peuvent être visionnées sur la chaine YouTube « African Cyber Security Summit » une fois mises en ligne.

Reference	ANPT-2019-BV-02
Titre	Bulletin de veille N°2
Date de version	26 juin 2019
Contact	ssi@anpt.dz