BULLETIN DE VEILLE N°5

ANPT-2019-BV-05

« Vous êtes un élément essentiel de nos efforts continus pour réduire les risques pour la sécurité.» -Kirsten Manthorne-

Septembre 2019

Alertes de sécurité

Microsoft

Multiples vulnérabilités dans les produits Microsoft

11 septembre 2019

De multiples vulnérabilités ont été découvertes dans les produits Microsoft. Elles permettent à un attaquant de provoquer un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et un déni de service.
Les produits affectés sont :

- Azure DevOps Server 2019
- ChakraCore
- Microsoft Exchange Server 2016 et 2019
- Microsoft Lync Server 2013
- Microsoft Visual Studio 2015, 2017 v 15.0 et v 15.9, 2019 v 16.0 et v 16.2
- Nuget 5.2.0
- Rome SDK 1.4.1
- Team Foundation Server 2015 Update 4.2, 2017 Update 3.1, 2018 Update 1.2 et 2018 Update 3.2
- Yammer pour Android

- Plusieurs versions de Windows 10, 32 et 64 bits
- Windows 7 SP1 32 et 64 bits
- Windows 8.1 32 et 64 bits
- Windows RT 8.1
- Plusieur versions de Windows Serveur 2008, 2012 et 2016

- NET Core 2.1 et 2.2
- ADAL.NET
- ASP.NET Core 2.1, 2.2 et 3.0
- Microsoft .NET Framework 3.5/ 4.6/ 4.6.1/ 4.6.2/ 4.7/ 4.7.1/ 4.7.2 / 4.8

- MS Office 2010, 2013, 2016 (32 et 64 bits)
- MS Project 2010, 2013 2016 (32 et 64 bits)
- MS SharePoint Entreprise server 2016, Foundation 2010 et 2013, Server 2019
- Office 365 ProPlus (32 et 64 bits)

Il est recommandé de se référer au bulletin pour plus de détails sur les différents correctifs.

Source *: https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-438/*
Bulletin *: https://portal.msrc.microsoft.com/fr-FR/security-guidance*

Multiples vulnérabilités corrigées dans Microsoft IE et Defender

23 septembre 2019

De multiples vulnérabilités ont été découvertes dans Microsoft Internet Explorer. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service. Une vulnérabilité de déni de service découverte quand Microsoft Defender traite de façon incorrecte les fichiers. Un attaquant pourrait exploiter cette vulnérabilité pour empêcher des comptes légitimes d'exécuter des binaires système légitimes.
Une mise à jour de sécurité cumulative a été publié pour corriger ces vulnérabilités.

Source : *https://nvd.nist.gov/vuln/detail/CVE-2019-1367*
https://nvd.nist.gov/vuln/detail/CVE-2019-1255
Bulletin : *https://portal.msrc.microsoft.com/fr-fr/security-guidance/advisory/CVE-2019-1367*

Mozilla

Multiples vulnérabilités dans Mozilla Firefox

04 septembre 2019

Plusieurs vulnérabilités ont été découvertes dans Mozilla Firefox et Firefox ESR (Extended Extended Release), la plus grave d'entre elles pouvant permettre l'exécution de code arbitraire.
En fonction des privilèges associés à l'utilisateur, un attaquant pourrait alors installer des programmes, afficher, modifier ou supprimer des données ; ou créer de nouveaux comptes avec des droits d'utilisateur complets. Les utilisateurs dont les comptes sont configurés avec moins de droits utilisateur sur le système

pourraient être moins impactés que ceux qui utilisent des droits d'administrateur.
Il est recommandé de mettre à jour l'application à sa version la plus récente.

Source : *http://bit.ly/2o3QQIr*

Google

Mise à jour Google Chrome corrige plusieurs failles de sécurité

19 septembre 2019

Une mise à jour massive de sécurité a été publiée pour le navigateur web Google Chrome corrigeant plusieurs failles de sécurité qui pouvaient permettre à un attaquant de contourner la politique de sécurité et atteindre à la confidentialité des données.
Les versions antérieures à 77 sont affectées. Il est recommandé d'appliquer les mises à jours disponibles sur le site officiel de l'éditeur.

Source : *https://chromereleases.googleblog.com/2019/09/stable-channel-update-for-desktop.html*

Linux

Multiples vulnérabilités dans le noyau de Red Hat

10 Septembre 2019

Dans ses deux bulletins de sécurité publiés le 10 septembre 2019, redhat déclare corriger de multiples vulnérabilités dans son noyau dont certaines permettent à un attaquant de provoquer des dénis de service, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.
Les correctifs appropriés sont listés pour chaque problème de sécurité dans le bulletin référencé.

Source : *https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-428/*

LibreOffice

Multiples vulnérabilités dans LibreOffice

06 septembre 2019

De multiples vulnérabilités ont été découvertes dans Libreoffice. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.
Les versions affectées : les versions antérieures à 6.2.7, les versions 6.3.x antérieures à 6.3.1.
Il est fortement recommandé de mettre à jour aux version les plus récentes afin de palier à ces vulnérabilités.

Source : *https://www.libreoffice.org/about-us/security/advisories/*

Vulnérabilité dans libreOffice

27 septembre 2019

Une vulnérabilité référencée CVE-2019-9853, a été découverte dans LibreOffice exploitant la manière dont les URL des macros sont traitées.
En effet, des documents peuvent contenir des macros dont l'exécution est contrôlée par les paramètres de sécurité du document. Généralement, l'exécution des macros est désactivée par défaut. Cependant, un défaut de décodage de l'URL existait donnant la possibilité de concevoir un document ou l'exécution de ses macros contournait les paramètres de sécurité.
Les documents sont correctement détectés comme contenant des macros mais ces dernières ne sont pas contrôlées ce qui offrirait la possibilité d'exécution de code arbitraire.
Il est recommandé de mettre à jour l'application.

Source : *https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-471/*
Bulletin : *https://www.libreoffice.org/about-us/security/advisories/cve-2019-9853/*

Cisco

Vulnérabilité dans le module Industrial Network Director (IND) de Cisco

04 septembre 2019

Une vulnérabilité dans le composant de services "plug-and-play" de Cisco Industrial Network Director (IND) pourrait permettre à un attaquant distant non authentifié d'accéder à des informations sensibles sur un périphérique affecté.
La vulnérabilité est due à des restrictions d'accès inappropriées sur l'interface Web de gestion. Un attaquant pourrait exploiter cette vulnérabilité en envoyant une requête HTTP à un périphérique affecté. Un exploit réussi pourrait permettre à l'attaquant d'accéder aux informations de configuration en cours d'exécution sur les périphériques gérés par l'IND, y compris les identifiants administratifs.
Cisco a publié des mises à jour logicielles qui répondent à cette vulnérabilité.

Source : *http://bit.ly/2ocQ5gx*

Vulnérabilité provoquant un déni de service dans les produits Cisco

17 Septembre 2019

Une vulnérabilité (CVE-2016-1409) dans les fonctions de traitement de paquets IPv6 de plusieurs produits Cisco pourrait permettre à un attaquant distant non authentifié d'empêcher un périphérique affecté de traiter le trafic IPv6, entraînant un déni de service (DoS) sur ce périphérique.
La vulnérabilité est due à une logique de traitement insuffisante pour les paquets IPv6 qui sont envoyés à un périphérique affecté. Un attaquant pourrait exploiter cette vulnérabilité en envoyant des paquets IPv6 Neighbor Discovery (ND) à un périphérique affecté pour traitement. Un exploit réussi pourrait permettre à l'attaquant d'empêcher le périphérique de traiter le trafic IPv6.
Selon le bulletin officiel, Cisco publiera des mises à jour logicielles qui répondent à cette vulnérabilité.

Systèmes affectés : tous les produits Cisco dont ipv6 est activée

Détail CVE : *http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1409*
Source : *http://bit.ly/2ntdN7G*

Wireshark

Multiples vulnérabilités dans Wireshark

12 septembre 2019

De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service à distance.
Systèmes affectés : Wireshark versions antérieures à 2.6.11 et version 3.0.X antérieures à 3.0.4.

Il est recommandé de mettre à jour l'application vers les versions 3.0.4, 2.6.11 ou ultérieure pour éliminer les vulnérabilités.

Source *https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-443/*
Bulletin : *https://www.wireshark.org/security/wnpa-sec-2019-21.html*

PhpMyAdmin

Vulnérabilité CSRF dans PhpMyAdmin

20 Septembre 2019

Une faille, de référence CVE-2019-12922, a été découverte dans PhpMyAdmin permettant une attaque de type Cross-Site Request Forgery contre un utilisateur phpmyadmin en supprimant un serveur dans la page Setup.
La faille a reçu un score de sévérité moyen vu sa portée limitée qui permet uniquement au pirate de supprimer un serveur configuré dans la page d'installation d'un tableau de bord phpMyAdmin.
Les versions impactées sont phpmyadmin antérieur à 4.9.0.1. Il est recommandé de mettre à jour l'application pour palier à la vulnérabilité.

Détail CVE : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12922
Source : https://meterpreter.org/cve-2019-12922-0-day-phpmyadmin/

Vmware

Multiples vulnérabilités dans les produits VMware

25 septembre 2019

De multiples vulnérabilités ont été découvertes dans les produits VMware, notamment ESXi, vCenter, Workstation et d'autres. Ces vulnérabilités permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité, un déni de service et escale de privilèges.
Trois bulletins datant du 17, 19 et 25 septembre détails les différentes vulnérabilités et les correctifs correspondants.

Bulletins : *https://www.vmware.com/security/advisories/VMSA-2019-0013.html*
https://www.vmware.com/security/advisories/VMSA-2019-0014.html
https://www.vmware.com/security/advisories/VMSA-2019-0015.html

Lenovo

Une vulnérabilité de déni de service dans Lenovo

24 septembre 2019

Une vulnérabilité de déni de service, référencée CVE-2019-6175, a été signalée dans Lenovo System Update qui pourrait permettre l'écriture de fichiers de configuration dans des emplacements non standard.
Les produits impactés sont :

- Lenovo 3000 C100, C200, N100, N200, V100, V200
- Lenovo 3000 J100, J105, J110, J115, J200, J200p, J205, S200, S200p, S205
- All ThinkPad
- All ThinkCentre
- All ThinkStation
- Lenovo V/B/K/E Series

Il est recommandé de mettre à jour à la version 5.07.0088 ou plus récente.

Détail CVE : *https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-6175*
Source : *https://support.lenovo.com/us/fr/solutions/len-28093*

Actualité

Google Play Store et Malware

24 septembre 2019

Google Play Store a souvent été sous les feux des projecteurs ces derniers temps à cause de problèmes d'hébergement d'applications malveillantes.

Des applications dont le téléchargement peut atteindre les millions, représentant ainsi une énorme menace pour un nombre considérable d'utilisateurs.

Parmi les applications approuvées par Google qui se sont avérées malveillantes :

Juin 2019 : environ 205 applications malveillantes auraient été téléchargées plus de 32 millions de fois en juillet seulement. Ces applications contenaient des codes malveillants permettant l'exploitation de portes dérobées, d'escroqueries d'abonnement, et plus encore.

Août 2019 : un outil populaire de générateur de fichiers PDF appelé CamScanner a été découvert pour contenir un module malveillant appelé 'Trojan-Dropper.AndroidOS.Necro.n'. Il a été observé que le module affichait des publicités intrusives. Après que Kaspersky l'ait signalé à Google, l'application a été immédiatement supprimée.

Septembre 2019 : ce mois-ci a vu la découverte d'une nouvelle campagne malveillante visant à propager le cheval de Troie Joker. Google a rapidement supprimé les 24 applications qui cachaient du code malveillant dans le framework de la publicité.

Google a supprimé deux applications de publicité, Sun Pro Beauty Camera et Funny Sweet Beauty Selfie Camera, qui ont totalisé plus de 1,5 million de téléchargements. De plus, quatre applications VPN - HotSpotVPN, Free VPN Master, Secure VPN et CM Security Applock AntiVirus - ont également été classées malveillantes.

Rien qu'en septembre 2019, 25 applications malveillantes totalisant 2,1 millions de téléchargements ont été observées diffusant des annonces aléatoires pour générer des revenus. Cependant, Google Play Store reste l'endroit le plus sûr pour télécharger des applications Android, mais avec autant d'incidents signalés, les utilisateurs sont invités à être en alerte. Aucune application n'est totalement à l'abri d'être exploitée à des fins malveillantes.

Assurez-vous de suivre les mesures de sécurité basiques, à savoir l'installation d'un antivirus, la mise à jour régulière des applications et la vérification des permissions demandées par les applications.

Source : *https://cyware.com/news/google-play-store-and-malware-a-recent-history-0e7546a9*

99 % des erreurs de configuration dans le cloud public ne sont pas signalées

25 septembre 2019

McAfee indique que ces incidents exposent les entreprises du monde entier à la perte et au vol de données.

De nos jours, les atteintes à la protection des données semblent souvent être causées non seulement par des infections de logiciels malveillants, mais aussi par des erreurs humaines. Certaines entreprises tentent d'ignorer les divulgations et les responsables des fuites de données, tandis que d'autres agissent rapidement lorsque l'information est rendue publique, et que leur réputation est en jeu.

La montée en flèche de l'adoption des technologies de cloud computing et de l'infrastructure-as-a-Service (IaaS) a ajouté une nouvelle facette aux cybermenaces - la perte d'information causée par les erreurs de configuration et la faiblesse des compétences dans le domaine de la gestion des cloud publics. Selon une nouvelle étude publiée mardi et menée par l'entreprise de cybersécurité McAfee, intitulée "Cloud-Native : The Infrastructure-as-a-Service Adoption and Risk", la majorité des erreurs de configuration sur les instances en mode IaaS passent inaperçues. En effet, seulement 1% des problèmes IaaS sont rapportés, ce qui peut suggérer qu'il y a d'innombrables entreprises à travers le monde qui laissent fuiter des torrents de données sans le vouloir...et sans le savoir.

1 000 professionnels de l'informatique ont été interrogés dans 11 pays, et les données sur l'utilisation du cloud de plus de 30 millions d'utilisateurs de McAfee Mvision ont été agrégées afin de compiler le rapport. Ce dernier indique également que les entreprises estiment avoir en moyenne 37 problèmes de mauvaise configuration IaaS par mois, ce qui en réalité peut atteindre 3 500 dans certains cas.

Source *: http://bit.ly/2o0wvDP*

Le compte du PDG de Twitter piraté dans un système d'échange de cartes SIM

02 septembre 2019

Des pirates ont brièvement repris le compte de Jack Dorsey, PDG de Twitter, tweetant des alertes à la bombe et des messages racistes et servant de rappel de la facilité avec laquelle il est possible de compromettre la sécurité.

"Le numéro de téléphone associé au compte a été compromis en raison d'un oubli de sécurité de la part du fournisseur de services mobiles" a déclaré Twitter vendredi dernier. Cela permettrait à une personne non autorisée de composer et d'envoyer des tweets par SMS à partir du numéro de téléphone. Ce problème est maintenant résolu.

Il a notamment été annoncé que "Rien n'indique que les systèmes de Twitter ont été compromis."

Cet incident est un parfait exemple des risques associés à la communication – toute forme de communication – lorsque l'identité de l'expéditeur n'est pas authentifiée. [..] Il a été prouvé qu'il existe des moyens très faciles de subvertir l'authentification à deux facteurs en incitant les agents des opérateurs à transférer le numéro de téléphone d'un utilisateur sur une nouvelle carte SIM ou en soudoyant un de ces agents.

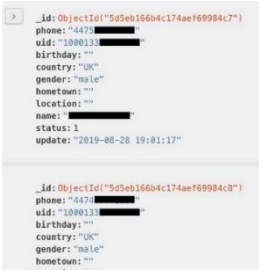
Alors que les tweets usurpés envoyés par le compte du PDG de Twitter sont offensants, ils demeurent bénins. Cependant des dégâts bien plus importants peuvent être faits via des techniques similaires. On le voit de plus en plus avec la communication par courriel. Un pirate informatique utilise l'usurpation d'identité pour envoyer des courriels d'hameçonnage extrêmement convaincants à un employé de l'entreprise, et en un rien de temps, de fausses factures sont payées, les données des consommateurs sont exposées, des virements électroniques sont faits à de fausses entreprises - la liste est sans fin.

[..] Il devient primordial de mettre l'accent sur la validation et l'authentification de l'identité de l'expéditeur, quelle que soit la forme de communication.

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

Une énorme base de données de numéros de téléphone d'utilisateurs Facebook trouvés en ligne

04 septembre 2019



Des centaines de millions de numéros de téléphone liés à des comptes Facebook ont été trouvés en ligne.

Le serveur exposé contenait plus de 419 millions d'enregistrements répartis sur plusieurs bases de données d'utilisateurs, dont 133 millions d'utilisateurs de Facebook aux États-Unis, 18 millions d'utilisateurs du Royaume-Uni et un autre de plus de 50 millions d'utilisateurs du Vietnam.

Le serveur n'étant pas protégé par mot de passe, la base de données était effectivement accessible au public – à tout utilisateur lambda.

Chaque enregistrement contenait l'ID Facebook unique d'un utilisateur et le numéro de téléphone figurant sur le compte. L'ID Facebook d'un utilisateur est généralement un numéro long, unique et public associé à son compte, qui peut être facilement utilisé pour discerner le nom d'utilisateur d'un compte. […]

Cet incident a ainsi divulgué des millions de numéros de téléphone d'utilisateurs uniquement à partir de leurs identifiants Facebook, les exposant ainsi au risque d'appels non sollicités ou d'attaques pouvant forcer la réinitialisation du mot de passe sur tout compte internet associé à ce numéro.

Source *: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/*

Microsoft : De nouveaux logiciels malveillants Nodersok ont infecté des milliers de PC

26 septembre 2019

Des milliers d'ordinateurs Windows à travers le monde ont été infectés par une nouvelle souche de logiciels malveillants qui télécharge et installe une copie du framework Node.js pour convertir les systèmes infectés en proxies et effectuer une fraude par clic.

Le maliciel, nommé Nodersok (dans un rapport Microsoft) et Divergent (dans un rapport Cisco Talos), a été détecté pour la première fois au cours de l'été et distribué par le biais de publicités malveillantes qui téléchargeaient de force des fichiers HTA (application HTML) sur les ordinateurs des utilisateurs.

Les utilisateurs qui ont trouvé et exécuté ces fichiers HTA ont lancé un processus d'infection en plusieurs étapes impliquant des scripts Excel, JavaScript et PowerShell qui ont finalement téléchargé et installé le malware Nodersok.
Le logiciel malveillant lui-même comporte plusieurs composants, chacun ayant son propre rôle. Il y a un module PowerShell qui essaie de désactiver Windows Defender et Windows Update, et il y a un composant pour élever les permissions du malware au niveau SYSTEM.

Mais il y a aussi deux composants qui sont des applications légitimes -- à savoir WinDivert et Node.js. Le premier est une application ayant pour but de capturer et d'interagir avec les paquets réseau, tandis que le second est un outil de développement bien connu pour exécuter JavaScript sur les serveurs Web.

[..] Comme toute autre souche de logiciel malveillant reposant sur une architecture client-serveur, les créateurs de Nodersok peuvent, à tout moment, déployer d'autres modules pour effectuer des tâches supplémentaires, ou même déployer des charges utiles secondaires de logiciel malveillant comme des logiciels en rançon ou des chevaux de Troie bancaires.

Pour prévenir les infections, le meilleur conseil est de ne lancent aucun fichier téléchargé à partir d'une page Web à la volé.

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

Microsoft Blacklists des dizaines de nouvelles extensions de fichiers dans Outlook

27 septembre 2019

Microsoft a interdit près de 40 nouveaux types d'extensions de fichiers sur sa plate-forme de messagerie Outlook, totalisant un nombre de 142 extensions. L'objectif est de protéger les utilisateurs de courriels contre ce qu'ils considèrent comme des pièces jointes "à risque", qui sont généralement envoyées avec des scripts ou des exécutables malveillants.
La mise en quarantaine empêchera les utilisateurs de télécharger des pièces jointes de courriel avec diverses extensions de fichiers, y compris celles associées à Python, PowerShell, certificats numériques, Java et plus encore. La liste complète se trouve ici.
Microsoft a déclaré que beaucoup de ces types de fichiers nouvellement bloqués sont rarement utilisés, de sorte que la plupart des organisations ne seront pas affectées par le changement : "Cependant, si vos utilisateurs envoient et reçoivent des pièces jointes affectées, ils signaleront qu'ils ne sont plus en mesure de les télécharger," dit-il.
Diverses extensions utilisées par des applications vulnérables seront également bloquées, qui pourraient être utilisées pour exploiter les vulnérabilités de sécurité des logiciels tiers, notamment : ".app-content-ms", ".settingcontent-ms", ".cnt", ".cnt", ".hpj", ".website", ".webpnp", ".mcf", ".printerexport", ".pl", ".theme", ".vbp", "xbap", ".xll", ".xnk", "msu", ".diagcab", ".grp"

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

Microsoft, la Fondation Hewlett et MasterCard lancent le CyberPeace Institute

09 septembre 2019

Microsoft, la Fondation Hewlett, MasterCard et plusieurs autres grandes entreprises et institutions philanthropiques anonymes ont créé une organisation indépendante à but non lucratif appelée CyberPeace Institute. Le but de celui-ci sera de protéger les victimes contre les cyberattaques et de les aider à s'en remettre.
L'Institute, qui sera initialement financé par les entreprises et les organisations philanthropiques concernées, se concentrera sur trois domaines d'activité principaux : Aider à coordonner les efforts de rétablissement des victimes de cyberattaques et aider les communautés et les organisations à devenir plus résilientes face aux attaques ; faciliter l'analyse collective, la recherche et les enquêtes sur les cyberattaques, y compris l'évaluation de leurs dommages pour apporter une plus grande transparence au problème ; et promouvoir un comportement responsable dans le cyberespace, et promouvoir les lois et règles internationales en la matière.

[..] Cette initiative collective fait suite à la décision de Microsoft, Facebook, Twitter et YouTube de restructurer un forum antiterroriste en ligne plus tôt cette semaine pour en faire une organisation indépendante dans le cadre des efforts de lutte contre le terrorisme sur les plateformes en ligne.

Le Global Internet Forum to Counter Terrorism (GIFCT), créé en 2017, a annoncé qu'il mettrait l'accent sur une coopération accrue entre les entreprises, les organismes gouvernementaux et les experts. La décision de faire de la GIFCT un organisme indépendant a été prise lors d'une réunion tenue lundi à l'Assemblée générale des Nations Unies pour discuter des prochaines étapes de l'appel de Christchurch.

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

Instagram : Les photos privées ne le sont pas vraiment

11 septembre 2019

Sur Instagram, les photos postées en mode privé et les stories ne le sont pas vraiment en réalité.

Qu'il s'agisse d'Instagram ou de Facebook, les publications privées permettent (en théorie) de limiter l'accès de certains contenus aux utilisateurs autorisés. La promesse d'une vie privée maîtrisée ? Pas vraiment. Il y a quelques jours, le site ***Buzzfeed*** a en effet rappelé qu'**il était très facile d'obtenir l'URL publique d'une publication privée**. Il suffit pour une personne ayant accès à un post ou à une vidéo story privée, de se rendre sur la page cible, et de faire un clic droit sur "Afficher le code source de la page". Quelques compétences très basiques en HTML suffisent ensuite pour trouver le lien direct du contenu recherché, qui peut alors être partageable à n'importe qui. La protection de la vie privée commence par la conscience de tout utilisateur des données privées qu'il consent à partager.

Source *http://bit.ly/2IYSwm3*

WhatsApp : La fonction « Supprimer pour tout le monde » ne supprime pas les fichiers multimédia envoyés aux utilisateurs d'iPhone

16 septembre 2019

Il s'avère que la fonction "Supprimer pour tout le monde" de WhatsApp ne supprime pas les fichiers multimédias envoyés aux utilisateurs de l'iPhone (avec les paramètres par défaut) comme ils le font à partir des appareils Android, laissant ainsi les fichiers envoyés sauvegardés sur l'appareil iOS du destinataire même si l'écran de la messagerie instantanée vous affiche, "Ce message a été supprimé."

La fonctionnalité de WhatsApp pour iOS n'a pas été conçue pour supprimer les fichiers multimédias reçus enregistrés dans la galerie de l'iPhone.

Source *:https://thehackernews.com/2019/09/whatsapp-delete-for-everyone-privacy.html*

Evènements

Evènements du mois

AI Hack

20-22 septembre 2019, Tunisie

Un hackathon organisé en Tunisie par InstaDeep et financé par le géant américain de l'internet Google, a réuni des centaines d'ingénieurs de la région Moyen-Orient et Afrique du Nord autour de plusieurs compétitions.

Il s'agit d'un double hackathon : la première partie est un défi individuel d'apprentissage automatique et la seconde partie est une compétition de groupe axée sur une technologie spécifique. Avec des mentors, des juges et des compétiteurs du monde entier.

La première place a été décrochée par l'équipe algérienne, **Alphateam**, et son projet baptisé **«YouNo solution»**. Une autre équipe algérienne a remporté la troisième place grâce à un projet dédié au domaine de l'éducation.

CONGRES SUR LA CYBERSECURITE ET LA PROTECTION DES DONNEES DANS L'INDUSTRIE PHARMACEUTIQUE ET DES SOINS DE SANTE, LONDRE

25-26 septembre 2019

Oxford Global a présenté le congrès sur la cybersécurité et la protection des données dans l'industrie pharmaceutique et des soins de santé. Plus de 450 participants représentant des sociétés pharmaceutiques mondiales, des sociétés de biotechnologie de premier plan et des établissements universitaires de renommée internationale. Le sujet portait sur la Cybersécurité, Stratégie de cybersécurité, Protection des données, Normes de cybersécurité, Gestion des données, Conformité des données, Résilience des données, Politique numérique et Gestion des risques.

Infos ANPT

Publication de la politique Générale de Sécurité des Systèmes d'Information **(PGSSI)** de l'ANPT

30 septembre 2019

A télécharger ici

http://bit.ly/2nFlXd4

Lancement d'une campagne de sensibilisation portant sur les bonnes pratiques de sécurité relatives aux postes de travail,

16 septembre 2019

Reference	ANPT-2019-BV-05
Titre	Bulletin de veille N°5
Date de version	30 septembre 2019
Contact	ssi@anpt.dz