BULLETIN DE VEILLE N°7

ANPT-2019-BV-07

« La confiance dans la technologie est une bonne chose, mais le contrôle est meilleur.» - Stephane Nappo-

Novembre 2019

Alertes de sécurité

Android

Multiples bugs traités dans les correctifs de sécurité Android

07 novembre 2019

Les correctifs de sécurité Android du mois de novembre ont corrigé un nombre important de bugs. Une exploitation réussie de la plus grave de ces vulnérabilités pourrait permettre l'exécution de code arbitraire dans le contexte d'un processus privilégié. Ces vulnérabilités pourraient être exploitées via plusieurs méthodes, telles que la messagerie électronique, la navigation sur le Web et MMS lors du traitement de fichiers multimédias.

Toutes les versions d'Android sans le correctif de sécurité 2019-11-01 et 2019-11-05 sont affectées. Il est fortement recommandé d'appliquer les mises à jour.

Source : *https://source.android.com/security/bulletin/2019-11-01*

WhatsApp

WhatsApp corrige une importante faille de sécurité

18 novembre 2019

WhatsApp, l'application de messagerie instantanée, a récemment corrigé une vulnérabilité impliquant l'utilisation des fichiers vidéo MP4 malveillants. Appelé débordement de pile-tampon identifiée par CVE-2019-11931.

La faille qui pourrait être exploitée avec des fichiers vidéo MP4 malveillants pourrait permettre à un attaquant d'accéder à distance aux messages et aux fichiers stockés dans l'application. Les fichiers vidéo malveillants sont utilisés pour exécuter à distance un code malveillant sur le périphérique de la victime sans aucune intervention.

Facebook, le propriétaire de WhatsApp, a en outre précisé dans son bulletin que cela pourrait également entraîner une attaque par déni de service (DoS).

Les versions affectées sont : les versions Android avant 2.19.274, les versions iOS avant 2.19.100, versions Enterprise Client avant 2.25.3, les versions de Windows Phone avant et y compris 2.18.368, Business pour les versions Android avant 2.19.104 et les versions Business pour iOS antérieures à 2.19.100.

Il est recommandé d'appliquer la dernière mise à jour publiée sur le site de l'éditeur.

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

Intel

Intel a corrigé 77 vulnérabilités

14 novembre 2019

Intel corrige 77 vulnérabilités, dont plus de deux douzaines étaient de gravité élevée et présentaient des failles de sécurité critiques affectant Windows et Linux.

La vulnérabilité CVE-2019-0169 a été caractérisée par le score de criticité le plus élevée, un dépassement de tampon susceptible d'entraîner une élévation de privilèges, une divulgation d'informations ou un déni de service sur les périphériques dotés d'Intel CSME avant les versions 11.8.70, 11.11.70, 11.22.70, 12.0.45 ou Intel Trusted Execution. Moteur (TXE) avant les versions 3.1.70 et 4.0.20.

Le fabricant recommande aux utilisateurs d'Intel CSME et de TXE de mettre à jour la dernière version fournie par le fabricant du système afin de résoudre le problème dès que possible. Une nouvelle vulnérabilité spéculative appelée ZombieLoad 2, trouvée dans le TAX (TSX Asynchronous Abort) et visant la fonctionnalité Transactional Synchronization Extensions (TSX) dans les processeurs Intel, a également été corrigée. La vulnérabilité CVE-2019-11135 pourrait permettre à un

attaquant authentifié localement de divulguer des informations sensibles.

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

Linux

Red Hat réagit aux vulnérabilités d'Intel.

13 novembre 2019

Suite aux vulnérabilités d'Intel, Red Hat annonce des mises à jour de sa distribution Linux pour résoudre les problèmes de processeur Intel susceptibles de conduire à différents exploits.

De nouvelles versions du noyau Linux ont été publiées afin d'atténuer ces nouvelles vulnérabilités de sécurité affectant les processeurs Intel. Elles devraient donc bientôt être disponibles dans les référentiels de logiciels stables de votre distribution GNU / Linux préférée. Red Hat recommande à tous les utilisateurs de mettre à jour leurs systèmes le plus rapidement possible, même s'ils ne croient pas que leur configuration constitue une menace directe.

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

Google

Correctif de vulnérabilité WebAudio Chromium

04 novembre 2019

Le 31 octobre 2019, Google a publié un correctif pour Google Chrome afin de corriger la sévère vulnérabilité de type zero-day référencée CVE-2019-13720 liée à la composante audio de Google Chrome.

L'exploit a été détecté par Kaspersky grâce au produit Kaspersky Exploit Prevention. Un programme malveillant permettant à des attaquants d'obtenir un accès non autorisé et d'avoir l'autorisation de lire et d'écrire des données sur l'ordinateur, qui peut conduire à une exécution de code arbitraire. Un acteur pourrait exploiter cette vulnérabilité en créant une page Web malveillante tirant parti du composant vulnérable de Chrome, puis en incitant les utilisateurs à consulter la page Web.

Google a publié des mises à jour qu'il est recommandé d'appliquer manuellement. Pour ce faire, cliquez sur les trois points verticaux situés dans le coin supérieur droit du navigateur : Personnaliser et contrôler Google Chrome -> sélectionnez Aide -> À propos de Google Chrome.

Source : https://www.kaspersky.com/blog/google-chrome-zeroday-wizardopium/29126/
Exploit : http://bit.ly/2OIF2VA

Google a résolu une vulnérabilité XSS dans Gmail

18 novembre 2019

La faille de sécurité était présente dans AMP4Email. Celui-ci, également appelé courrier électronique dynamique, a été mis en œuvre pour faciliter l'affichage du contenu dynamique dans les courriers électroniques, tels que les fils de commentaires ou les invitations à des événements.

Le 15 août 2019, la vulnérabilité avait été signalée via le programme de vulnérabilité de Google.

Un jour plus tard, l'équipe de Google avait accepté le rapport. Le 10 septembre, elle avait déclaré : "Le bug est *awesome*, merci de nous l'avoir signalé !"

Le 12 octobre, le géant de la technologie a informé Bentkowski que le problème avait été résolu, ce qui avait conduit à une déclaration publique.

Source : https://www.zdnet.com/article/google-patches-awesome-xss-vulnerability-in-gmail/

Adobe

Adobe corrige des bugs critiques d'exécution de code à distance dans Illustrator

12 novembre 2019

Adobe a publié des mises à jour de sécurité pour résoudre les problèmes permettant à des attaquants d'exécuter du code malveillant, d'élever des privilèges et d'obtenir un accès non autorisé à des informations sur des systèmes exécutant des versions non corrigées d'Illustrator, Animate CC, Bridge CC et Media Encoder.

Deux vulnérabilités nommées CVE-2019-8247 et CVE-2019-8248 sont considérées critiques. L'exploitation réussite de la corruption de mémoire conduit à l'exécution de code à distance dans le logiciel Adobe Illustrator.

Il est recommandé d'appliquer la mise à jour de la dernière version (24.0) du logiciel.

Source : https://threatpost.com/adobe-critical-bugs-illustrator-media-encoder/150114/

Vmware

Trois Vulnérabilités dans les produits VMware

13 novembre 2019

VMware a diffusé 3 vulnérabilités jugées importantes qui sont CVE-2019-5540, CVE-2019-5541 et CVE-2019-5542 affectant les plateformes : VMWare Workstation version 15.x antérieure à 15.5.1, VMWare Fusion version 11.x antérieure à 11.5.1, VMWare ESXi version 6.0.x, 6.5.x, 6.7.x.

CVE-2019-5541 entraîne l'exécution de code sur l'hôte à partir de l'invité ou permettre aux attaquants de provoquer un déni de service sur leur propre ordinateur virtuel. CVE-2019-5540 permet à un attaquant, sur une machine virtuelle, de divulguer des informations sensibles récupérées à partir de la mémoire du processus hôte. CVE-2019-5542 fait référence à une vulnérabilité de déni de service dans le gestionnaire RPC, qui permet aux attaquants disposant des privilèges utilisateurs normaux de provoquer un déni de service sur leur propre ordinateur virtuel.

Des correctifs pour toutes les vulnérabilités sont disponibles sur le site officiel de l'éditeur.

Source : http://bit.ly/2D8OTie
Détails CVE : http://bit.ly/2ObIk3k, http://bit.ly/2KSOMry, http://bit.ly/2QQfpoM

Microsoft

Vulnérabilité d'usurpation d'identité dans Outlook pour Android

19 novembre 2019

Il existe une vulnérabilité d'usurpation d'identité (CVE-2019-1460) dans la façon que Microsoft Outlook d'Android traite des messages électroniques spécialement conçus. Un attaquant authentifié pourrait exploiter cette vulnérabilité en envoyant un message électronique spécialement conçu (une injection de code indirecte à distance (XSS)) à une victime.

L'attaquant qui parviendrait à exploiter cette vulnérabilité pourrait ensuite mener des attaques entre sites sur les systèmes affectés et d'exécuter des scripts dans le contexte de sécurité de l'utilisateur actuel.

Source : *https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1460*

Microsoft corrige 74 failles du jour zéro d'IE

12 novembre 2019

Microsoft a publié des mises à jour pour 74 vulnérabilités. Parmi ces vulnérabilités, 13 sont classées comme critiques. La mise à jour a inclus le correctif pour la vulnérabilité zero-day intitulée CVE-2019-1429 permettant l'exécution de code à distance dans Internet Explorer.

Microsoft a également fixé une vulnérabilité révélée publiquement dans Microsoft Office pour Mac intitulé « CVE-2019-1457 Microsoft Office Excel qui permet aux pirates de contourner les restrictions de sécurité.

Tous les utilisateurs doivent installer ces mises à jour de sécurité le plus rapidement possible afin de protéger Windows des risques de sécurité connus.

Source :*https://www.bleepingcomputer.com/news/microsoft/microsofts-november-2019-patch-tuesday-fixes-ie-zero-day-74-flaws/*

BIND

Vulnérabilité dans BIND

20 novembre 2019

Une vulnérabilité nommée CVE-2019-6477 a été corrigée dans le DNS de BIND. Un attaquant pourrait exploiter cette vulnérabilité afin de provoquer un déni de service à distance.

Cette vulnérabilité peut être contournée en désactivant le TCP-pipelining sur le serveur.

Versions affectées : BIND 9.11.6-P1 à 9.11.12, 9.12.4-P1 à 9.12.4-P2, 9.14.1 à 9.14.7 et versions 9.11.5-S6 à 9.11.12- S1 de la version d'aperçu prise en charge par BIND 9. Les versions 9.15.0 à 9.15.5 de la branche de développement de BIND 9.15 sont également affectées.

Il est recommandé d'appliquer les mises à jour selon la version.

Source : *https://kb.isc.org/docs/cve-2019-6477*

Actualité

L'exploitation de BlueKeep est de retour par des cybercriminels

04 novembre 2019

Un groupe de hackers a utilisé un exploit Bluekeep de démonstration implémenté par l'équipe de Metasploit en septembre dernier pour pirater des systèmes Windows vulnérables et installer un mineur de cryptomonnaie.

Cette campagne d'attaques se déroule à grande échelle et dure depuis près de deux semaines, mais n'a été repérée que récemment par Kevin Beaumont, expert en cybersécurité.

L'expert en sécurité britannique explique avoir trouvé les exploits dans des journaux enregistrés par des réseaux honey pots qu'il avait mis en place des mois auparavant et qu'il avait oublié.

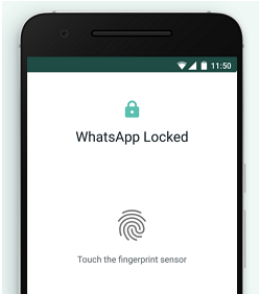
Les pirates semblent chercher des systèmes Windows avec des ports RDP laissés exposés sur Internet, déployer l'exploit BlueKeep Metasploit, et plus tard un mineur de cryptomonnaie.

Bien que cela fait des mois que le patch a été lancé, le nombre des systèmes Windows accessibles au public qui exposent un terminal RDP en ligne et qui sont vulnérables à BlueKeep est d'environ 750 000. Les correctifs sont disponibles depuis le mois de mai 2019.

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

WhatsApp inaugure le verrouillage biométrique pour Android

04 novembre 2019



WhatsApp a annoncé le déploiement de l'authentification biométrique via les capteurs d'empreintes digitales sur Android. Le 31 octobre 2019 Le groupe WhatsApp a déclaré que les appareils fonctionnant sous le système d'exploitation Android de Google, s'ils étaient d'un modèle suffisamment récent, pourront bientôt sécuriser l'accès à leur compte par cette méthode.

Pour activer la nouvelle option, les utilisateurs doivent naviguer sur Paramètres -> Compte -> Confidentialité -> Verrouillage par empreinte digitale. Si les utilisateurs choisissent d'activer la fonctionnalité, ils devront utiliser leur empreinte digitale pour ouvrir l'application.

Les utilisateurs peuvent également sélectionner le temps nécessaire pour que WhatsApp se verrouille, afin d'éviter de voir les notifications pour déverrouiller l'application dans son utilisation quotidienne. De plus, les appels téléphoniques ne seront pas bloqués par la fonction.

Au moment de la rédaction de cet article, la fonctionnalité ne semble pas être arrivée sur les appareils Samsung, mais attendez-vous à ce que celle-ci apparaisse bientôt.

WhatsApp a annoncé la prise en charge des outils d'authentification biométriques Touch ID et Face ID d'Apple

plus tôt cette année. Dans iOS 9 et les versions ultérieures, les utilisateurs d'iPhone peuvent activer les Touch ID et l'authentification via reconnaissance faciale en ouvrant WhatsApp et en naviguant jusqu'à Paramètres -> Compte -> Confidentialité -> Verrouillage de l'écran.

L'ajout de cette couche de sécurité biométrique fait suite à une apparition en bêta l'été dernier.

Source : *bhttp://bit.ly/2QSTDAG*

WP-VCD, la plus grande opération de piratage WordPress actuelle

07 novembre 2019

La principale menace visant les sites WordPress est une opération criminelle connue sous le nom de WP-VCD, actuellement responsable de la grande majorité des sites WordPress piratés.

Le groupe WP-VCD n'utilise pas de vulnérabilités pour pénétrer dans des sites et installer des backdoors. Au lieu de cela, ils comptent sur les erreurs des webmasters pour s'infecter eux même en téléchargeant et en installant des thèmes et des plug-ins piratés pour leurs sites WordPress, en proposant des téléchargements gratuits de thèmes commerciaux populaires, généralement vendus dans des magasins en ligne ou sur des sites populaires tels que ThemeForest ou CodeCanyon.

Parmi les sites de distribution de thèmes et de plug-ins piégés :

download-freethemes.download, downloadfreethemes.space, downloadnulled.pw, downloadnulled.top, freenulled.top, nulledzip.download, themesfreedownload.net, themesfreedownload.top, vestathemes.com.

Ces sites se classent bien dans les résultats de recherche sur les moteurs de recherche (parmi les 3 premiers résultats), afin d'avoir un maximime de chances d'être exploités.

Les propriétaires de sites WordPress doivent garder à l'esprit que, lorsque quelque chose est gratuit, "vous êtes le produit" – dans ce cas votre site – qui est utilisé par des cybercriminels.

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

Windows 7 et Windows server 2008 R2 : Quelles solutions pour passer le deadline du 14 janvier 2020 ?

07 novembre 2019

Une récente étude Ivanti montre que 59% des entreprises n'ont toujours pas migré l'ensemble de leur parc de PC Windows 7 vers Windows 10. A quelques semaines de la date de fin de support de l'OS commercialisé par Microsoft en 2009, 39% des professionnels de l'IT déclarent qu'ils n'auront certainement pas achevé leur migration d'ici 14 janvier 2020, date officielle de fin de support.

Beaucoup d'entre-elles vont se retrouver à gérer un parc de postes clients qui ne recevront plus de mise à jour de sécurité, ce qui, à l'heure des attaques de masses de malware est alarmant. Microsoft propose à ces retardataires plusieurs solutions pour étendre l'utilisation de Windows 7 et Windows server 2008 R2. La première est l'achat de l'extension de support (ESU, pour Extended Security Updates) sur 3 ans, une extension au prix qui accroitra année après année : la première année est facturée 25 $ par poste Windows Enterprise, puis 50 $ l'année suivante, puis 100 $ la troisième année. Ce tarif est doublé s'il s'agit de Windows 7 Pro. En outre, pour ceux qui voudront faire une mise à jour globale la troisième année, il leur faudra aussi payer les années 1 et 2 en rattrapage.

La seconde est une alternative qui propose l'offre de virtualisation du poste de travail dans le Cloud. « Windows Virtual Desktop : permet de bénéficier d'une expérience multiutilisateurs et qui inclut gratuitement les mises à jour de sécurité. On accède ainsi gratuitement à l'offre Extended Security Updates pendant un an » argumente le directeur technique de Microsoft.

Source : *bhttp://bit.ly/2XNQzaE*

Magecart, le groupe de pirates qui sème la terreur sur les sites de commerce en ligne.

04 novembre 2019

Le vol de données de cartes de paiement et de données personnelles sur des sites de commerce électronique est devenu si lucratif que certains sont ciblés par plusieurs groupes en même temps. Dans une évolution intéressante sur la scène de la cybercriminalité financière, différents groupes Magecart se sont aperçus qu'ils se superposaient et attaquaient les mêmes sites.

Magecart est un terme générique englobant plusieurs groupes de menaces qui utilisent tous le même mode opératoire : ils compromettent les sites Web construits sur la plateforme de commerce électronique Magento afin d'injecter des scripts très volumineux dans les pages de paiement, de voler les détails des cartes de paiement sans méfiance des clients et autres informations entrées dans les champs de la page.

Selon les recherches de PerimeterX, plusieurs attaques Magecart effleurent en même temps les cartes de crédit de sites. Celles-ci ne semblent pas être coordonnées, selon l'entreprise, étant donné que chacune des attaques était différente en termes de techniques utilisées pour compromettre les détaillants ciblés.

Afin de se protéger contre ce type d'attaque, il faut vérifier que votre plateforme e-commerce soit conforme avec le standard PCI DSS.

Source *: http://bit.ly/33iudz8*

Wizard Spider met à niveau Ryuk Ransomware pour atteindre les réseaux locaux

04 novembre 2019

Les commandes Wake-on-LAN (WoL) et Address Resolution Protocol (ARP) ont étendu la portée de Ryuk aux réseaux locaux d'entreprise et aux capacités de monétisation de ses opérateurs.

La première nouvelle fonctionnalité de Ryuk tente de réveiller les hôtes du réseau local qui sont en mode veille en leur envoyant un paquet magique WoL. La machine affectée doit prendre en charge WoL et sa carte réseau doit avoir le paramètre configuré dans le BIOS. Pour identifier les machines sur le réseau local, Ryuk lit les entrées du cache ARP de l'hôte. De plus, pour chaque adresse dans le cache, il envoie un paquet magique WoL. Le paquet est envoyé via un socket UDP (User Datagram Protocol) utilisant le port de destination 7. Cependant, les paquets ayant comme destination port 7 lors d'un incident lié au logiciel de rançon peuvent indiquer que Ryuk est présent.

La deuxième fonctionnalité de Ryuk utilise le scan de Ping ARP pour identifier les hôtes sur le réseau local.

Dans le but de détecter et prévenir contre les attaques de Ryuk, les paramètres de prévention doivent être définis au minimum sur les éléments suivants :

- Antivirus nouvelle génération: apprentissage à partir des données collectées du cloud et les capteurs: réglez le curseur «Prévention» sur «Modéré».
- Protection contre les programmes malveillants: Blocage d'exécution: Basculez : «Empêcher les processus suspects» sur «Activé».
- Ajoutez des hachages à votre liste noire personnalisée pour une protection accrue.

Source *: https://threatpost.com/wizard-spider-upgrades-ryuk-ransomware/149853/*

Abonnés Canal Plus changez votre mot de passe !

11 novembre 2019

Plusieurs milliers de comptes client **Canale plus** ont été exploités par un pirate pour les revendre à d'autre personnes. « La livraison se fait instantanément après votre paiement. Indique le pirate. Si vous ne recevez pas le compte, merci de vérifier dans vos spams/courriers indésirables. Si vous ne le trouvez pas, alors contactez-moi en me précisant le numéro de commande ». Le paiement se fait par Paypal. Le pirate précise qu'il ne faut pas modifier les informations du compte. Sans quoi la garantie ne sera pas valable.

Il a été soupsonné que les données des comptes ont été principalement volées en utilisant la technique du phishing.

Pour vous protéger contre cette éventuelle possibilité d'être piraté il est conseillé de changer immédiatement vos mots de passe : Cliquer sur « Mot de passe oublié » présent dans votre espace client. Changer le « précieux ». prenez garde à ne pas utiliser votre « prénom123 ».

Source *: https://www.zataz.com/clients-abonnes-canal-plus-changez-votre-mot-de-passe/*

Utilisateurs d'Android, méfiez-vous : 146 bugs détectés dans des applications préinstallées

15 novembre 2019

Le souci quand on achète un smartphone, c'est qu'on se retrouve bien souvent avec des dizaines d'applications préinstallées, le cabinet d'études sur la sécurité Kryptowire a, de nouveau, exposé toute une panoplie d'activités potentiellement malveillantes avec des applications préinstallées sur des téléphones Android peu coûteux . Dans le cadre d'une recherche financée par le US Department of Homeland Security, l'entreprise a découvert que des applications enregistraient en secret des données audio, modifiaient les paramètres du téléphone sans l'autorisation de l'utilisateur et s'octroyaient même de nouvelles autorisations.

Les applications préinstallées telles que celles trouvées dans les recherches de Kryptowire sont souvent de petits logiciels sans marque intégrés à des fonctions d'applications de marque plus grandes. Les applications préinstallées représentent une menace particulièrement grave pour la sécurité, car elles ont généralement plus de liberté d'utilisation que les autres types d'applications, et peuvent être plus difficiles à supprimer pour un utilisateur. Il est donc recommandé de désactiver ces applications en suivant ce processus : Parametre -> liste des application installées -> séléctionner une application -> appuier sur désactiver.

Source *: https://cnet.co/2Da88YD*

Un serveur Elasticsearch exposé contenant 1,2 milliard de données.

25 novembre 2019

Le serveur était accessible sans authentification et contenait 4 milliards de comptes utilisateur, couvrant plus de 4 téraoctets de données, ont découvert les chercheurs en sécurité Bob Diachenko et Vinny Troia le mois dernier.

L'analyse des données a révélé qu'elles concernaient plus de 1,2 milliard de personnes et qu'elles comprenaient des noms, des adresses électroniques, des numéros de téléphone, ainsi que des informations sur les profils LinkedIn et Facebook.

Une enquête plus approfondie a conduit les chercheurs à la conclusion que les données provenaient de deux sociétés d'enrichissement de données différentes. Ainsi, la fuite représente en fait des données agrégées provenant de diverses sources et mises à jour. […] Les chercheurs n'ont pas pu déterminer qui était responsable de laisser le serveur ouvert à Internet, mais ils ont suggéré qu'il s'agissait d'un client de People Data Labs et d'OxyData et que les données auraient peut-être été utilisées abusivement plutôt que volées. «Les nombreuses informations personnelles incluses, associées aux difficultés d'identification du propriétaire des données, peuvent potentiellement poser des questions sur l'efficacité de nos lois actuelles en matière de confidentialité et de notification d'infractions», concluent les chercheurs. ». […] Si un attaquant dispose d'un pareil ensemble de données, il peut formuler des attaques très ciblées. Les types d'attaques qui peuvent permettre de connaître les informations de récupération de mot de passe, les données financières, les modèles de communication, les structures sociales, sont les moyens par lesquels les personnes au pouvoir peuvent être ciblées et, au final, les attaques peuvent fonctionner.

Source *: https://www.securityweek.com/data-12-billion-users-found-exposed-elasticsearch-server*

Une nouvelle technique permet à Ransomware de fonctionner sans être détecté

25 novembre 2019

Une technique récemment découverte permet aux ransomwares de chiffrer des fichiers sur des systèmes Windows sans être détectés par les produits anti-ransomwares existants, préviennent les chercheurs en sécurité de Nyotron. Cette technique permet aux logiciels malveillants de contourner les défenses à l'aide de l'opération "renommer" du système de fichiers hérité. Les chercheurs en sécurité affirment qu'elle est efficace même si les systèmes sont patchés et dispose des solutions antivirus modernes. […] Les chercheurs ont découvert la technique au printemps 2019 et ont été en contact avec Microsoft, des fournisseurs de sécurité et des autorités chargées de l'application de la loi. Malheureusement, ils affirment que peu de fournisseurs de sécurité ont su trouver une solution pour résoudre les problèmes.

Source : *https://www.securityweek.com/new-technique-allows-ransomware-operate-undetected*

Informations de commande des clients OnePlus exposés à une violation de données

25 novembre 2019

Le fabricant chinois de smartphones OnePlus a révélé vendredi que les informations de commande de certains clients avaient été consultées par des pirates informatiques qui avaient violé ses systèmes.

Selon la société, son équipe de sécurité a récemment remarqué un accès non autorisé aux informations de commande, notamment les noms, les numéros de téléphone, les adresses électroniques et les adresses d'expédition. L'incident ne semble pas avoir d'impact sur toutes les commandes et OnePlus est convaincu que les informations de paiement et les mots de passe n'ont pas été compromis. La société craint que les attaquants n'utilisent ces informations pour envoyer des e-mails de spam et de phishing, et a conseillé aux clients de ne pas faire confiance aux messages les invitant à fournir leur mot de passe ou leurs informations financières. […] La société envisage de lancer un programme officiel de primes de bogues d'ici la fin de l'année afin de l'aider à découvrir les failles de sécurité avant qu'elles ne soient exploitées à des fins malveillantes.

Source :*https://www.securityweek.com/order-information-oneplus-customers-exposed-data-breach*

Evènements

Evènements du mois

Grenoble INP organise un concours mondial de hacking, Valence

06-08 novembre 2019

http://esisar.grenoble-inp.fr/fr/l-ecole/inscriptions-csaw-19

L'école nationale supérieure en systèmes avancés et réseaux Grenoble INP – Esisar a organisé du 6 au 8 novembre à Valence l'édition européenne de la Cybersecurity awareness week (CSAW) 2019. Lancée en collaboration avec la New York University cette compétition a été mise sur pied pour susciter l'intérêt et les vocations des étudiants de tous niveaux (des lycéens aux doctorants) pour les métiers liés à la cyber-sécurité. Elle a proposé en plus de ses concours, des conférences thématiques ainsi qu'un forum industriel dédié à la cyber-sécurité.

Cyber Security Connect UK, Monaco

13-15 novembre 2019

https://www.cybersecurityconnectuk.com/

Cet événement s'est déroulé sur trois jours non-stop de réseautage et d'apprentissage dans un environnement fermé. Il a compris : des conférences, des discours, des discussions d'experts, des ateliers pour partenaires, mise en réseau des acteurs stratégiques du secteur de la cyber-sécurité (déjeuners et soirées VIP), réunions individuelles préprogrammées et ciblées avec des solutions de sécurité informatique et des fournisseurs de services sélectionnés.

Cloud and Cyber-Security Expo, Paris

27-28 novembre 2019

https://www.cloudexpoeurope.fr/csep/cloud--cyber-security-expo

250 experts de l'industrie issus de grandes entreprises françaises étaient présents lors d'études de cas, tables rondes et conférences spécialisées dans la sécurité, conformité et réglementation, sécurité des objets connectés, protection des données, sécurité des infrastructures, sécurité dans le cloud et bien plus encore, dans le but d'apprendre à mieux détecter, prévenir et gérer les multiples menaces en matière de cyber-sécurité

Reference	ANPT-2019-BV-07
Titre	Bulletin de veille N°7
Date de version	30 Novembre 2019
Contact	ssi@anpt.dz