BULLETIN DE VEILLE N°2

ANPT-2020-BV-02

«L'évolution numérique ne doit plus être offerte en échange avec la confidentialité et la sécurité du client...» - *Stephane Nappo-*

Février 2020

Alertes de sécurité

Réseaux sociaux

L'utilisation de WhatsApp sur votre ordinateur pourrait mettre vos fichiers en danger

06 février 2020

La chercheuse Gal Weizman de PerimeterX a trouvé une vulnérabilité JavaScript dans la plate-forme de bureau WhatsApp qui pourrait permettre aux cybercriminels d'accéder et lire les fichiers des victimes.

La vulnérabilité est apparue dans les versions Windows et Mac de l'application où elle gère les bannières ou les aperçus des liens Web dans les messages. Le code JavaScript attaché à une bannière malveillante pourrait contourner les mécanismes de protection et accéder au système de fichiers local de la victime.

Selon la chercheuse, le cœur de la faille réside dans le moteur de navigateur Chromium dans le cadre d'application Electron.

WhatsApp s'appuie sur elle pour fournir une interface utilisateur pour son client de bureau.

Bien que le bug XSS ait été corrigé plus tôt dans Chromium, WhatsApp a utilisé une ancienne version d'Electron pour Chromium.

Source : *http://bit.ly/2w5Qkhn*

Android

Un bug Bluetooth critique affectant la plupart des appareils Android

10 février 2020

Google a publié une mise à jour de sécurité pour corriger une faille critique dans l'implémentation Bluetooth d'Android. La vulnérabilité référencée CVE-2020-0022, affecte les appareils exécutant Android Oreo (8.0 et 8.1) et Pie (9.0) et peut permettre l'exécution de code à distance, aucune interaction utilisateur n'est requise et seule l'adresse MAC Bluetooth des appareils cibles doit être connue. La faille a été découverte et signalée à Google il y a trois mois par la firme de sécurité allemande ERNW et le correctif a été publié au début de ce mois. Cependant, tous les appareils non mis à jour restent vulnérables grâce à leur connectivité Bluetooth. En attendant que les fabricants déploient des mises à jour, une façon de réduire le risque est de vous assurer que votre téléphone est en mode non détectable lorsque le Bluetooth est activé. Alternativement, activez Bluetooth uniquement si nécessaire et n'oubliez pas de le désactiver lorsqu'il n'est pas utilisé.

Source : *http://bit.ly/39miuD1*

Google

Chrome 80 est disponible avec 56 correctifs de sécurité

07 février 2020

Google a publié le 04 février 2020 Chrome 80, la dernière version de son navigateur Web phare pour les utilisateurs de Windows, Mac, Linux, Android et iOS.

Chrome 80 vient avec 56 correctifs de problèmes de sécurité découverts par des chercheurs externes, dont certains «corrigent» des failles de sécurité dans JavaScript et plusieurs vulnérabilités dans XML.

La nouvelle version comprend également des améliorations de la sécurité des cookies, la gestion des icônes favorites basées sur SVG, la prise en charge de l'opérateur nul de JavaScript et WebVR 1.1.

La nouvelle la plus importante, cependant, est qu'avec Google Chrome v80, la prise en charge des extrémités FTP est désormais désactivée par défaut. Ceux qui ont besoin de continuer à utiliser le protocole peuvent le réhabiliter simplement en écrivant –enable-ftp à partir de la ligne de commande, mais Google prévoit de supprimer tout le code lié à FTP dans la version 82 du navigateur Chrome.

Source : *http://bit.ly/2OG5BvE*

Microsoft

Microsoft a publié des correctifs critiques pour février 2020

11 février 2020

Microsoft a publié des mises à jour du mois de février, corrigeant 99 vulnérabilités de sécurité. Parmi ces vulnérabilités, des bugs d'exécution de code à distance (RCE) dans SQL Server 2012, 2014 et 2016 (32 et 64 bits) et Windows 7, 8.1, 10, Server 2008, 2012, 2016 et 2019. En outre, deux vulnérabilités critiques d'exécution de code à distance dans Remote Desktop (CVE-2020-0681 et CVE-2020-0734) ont été corrigées et sont susceptibles d'être exploitées, selon Microsoft.

La mise à jour comprend un correctif pour la vulnérabilité zero-day référencée CVE-2020-0674 de corruption de mémoire, révélée fin janvier, qui fait l'objet d'une attaque active. Pour plus de détails, veuillez consulter la source.

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

Le dernier correctif de Windows 10 engendre un bug du profil utilisateur

14 février 2020

Microsoft a publié un correctif pour Windows 10 qui risquerait d'engendrer un bug embêtant. Les utilisateurs de Windows 10 ayant installés le dernier patch, KB4532693 ont rencontré un problème dans le chargement du profil utilisateur. Subitement, toutes les données disparaissent ainsi que tous les paramètres du système d'exploitation. Le dossier de profil utilisateur original a été renommé par Windows, et ce dernier a ensuite créé et chargé un profil utilisateur provisoire au démarrage de l'ordinateur.

L'utilisateur pourra trouver le profil original en se dirigeant vers C:\Users> et en cherchant un fichier renommé qui se termine par «.ooo» ou «.bak». L'utilisateur ne pourra accéder à son profil de cette manière, sauf que d'autres moyens de récupération existent. La solution est de désinstaller la mise à jour en attendant que Microsoft publie toutes les corrections nécessaires.

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

Firefox

La mise à jour du navigateur de Mozilla Firefox 73

12 février 2020

Mozilla a lancé les dernières versions Firefox 73 et Firefox ESR 68.5 de son navigateur Firefox, corrigeant les failles de sécurité très sévères qui laissent les systèmes ouverts aux attaques distantes. Les deux versions corrigent six vulnérabilités. Deux des bogues les plus graves permettent à un attaquant distant d'exécuter du code sur des appareils ciblés en incitant les utilisateurs à visiter un site Web spécialement conçu et en exploitant les failles de corruption de mémoire du navigateur.

Le bulletin de sécurité de Mozilla a déclaré que les deux failles de haute gravité sont liées à des «bugs de sécurité de la mémoire dans le moteur de navigateur». L'une des vulnérabilités, identifiée CVE-2020-6800 a été corrigée dans une version précédente de Firefox 72 et la mise à jour actuelle de Firefox ESR 68.5. L'autre vulnérabilité CVE-2020-6801 a été corrigée avec la sortie de Firefox 73.

Thunderbird 68.5.0 a également été publié. Dans le cadre de cette version, six failles de gravité moyenne et faible ont été corrigées (ainsi que CVE-2020-6800).

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

Linux

Une vulnérabilité critique dans systemd

11 février 2020

Tavis Ormandy, un chercheur chez Google Project Zero vient de signaler la découverte d'une vulnérabilité critique dans systemd, le sous- système d'initialisation Linux. Si elle est exploitée, la vulnérabilité permettrait à un acteur de la menace d'exécuter du code avec des privilèges d'administrateur sur le système affecté en envoyant des requêtes spécialement conçues via DBus. Selon le rapport, la faille, CVE-2020-1712, est présente dans Ubuntu, Red Hat, Fedora, RHEL, CentOS, SUSE / openSUSE et ROSA, et a reçu un score de 7,8 / 10 sur le score de vulnérabilité commun Échelle du système (CVSS).

À ce stade, seul Red Hat a pris position sur cette constatation.

Source : *http://bit.ly/2V1Rg0m*

WordPress

Des vulnérabilités critiques dans deux plug-ins WordPress

12,17 février 2020

Le plugin ThemeGrill Demo Importer possède plus de 200 000 installations actives et peut être utilisé pour importer le contenu, les widgets et les paramètres de thème officiels de ThemeGrill en un seul clic.

Dans les versions 1.3.4 et supérieures et les versions 1.6.1 et inférieures, il existe une vulnérabilité qui permet à tout utilisateur non authentifié d'effacer l'intégralité de la base de données à son état par défaut, après une authentification automatique en tant qu'administrateur. Sur la base de l'historique des validations SVN, ce problème existe dans le code depuis environ 3 ans, depuis la version 1.3.4. Il est recommandé aux utilisateurs de ce plug-in d'appliquer le **patch** dans les plus brefs délais.

Une autre vulnérabilité XSS critique corrigée dans le plugin WordPress GDPR Cookie Consent, le plugin est activement installé sur plus de 700 000 sites Web. Des charges utiles malveillantes peuvent alors être exécutées et se chargent lorsque *http://nom_du_site_web/cli-policy-preview/* est visité par des membres du public. Il est recommandé aux utilisateurs du plugin GDPR Cookie Consent de s'assurer qu'ils utilisent la dernière version du logiciel, 1.8.3.

Source : *http://bit.ly/39Oom83 ; https://zd.net/2SBULsM*

Cisco

5 vulnérabilités zero-day dans le protocole CDP

06 évrier 2020

Cisco a publié des correctifs pour cinq vulnérabilités critiques affectant le Cisco Discovery Protocol (CDP). Les cinq vulnérabilités, collectivement appelées CDPwn, découvert par

des chercheurs d'Armis, peuvent permettre à un attaquant de prendre entièrement le contrôle des appareils ciblés. Les vulnérabilités ont été révélées à Cisco le 29 août 2019.

Quatre des cinq vulnérabilités référencées CVE-2020-3119, CVE-2020-3118, CVE-2020-3111, CVE-2020-3110 sont des vulnérabilités d'exécution de code à distance (RCE) et la dernière référencée CVE-2020-3120 est une vulnérabilité de déni de service (DoS). Les mises à jour pour chaque vulnérabilité peuvent être trouvées respectivement ici : 1 ; 2 ; 3 ; 4 ; 5.

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

IBM

Vulnérabilité critique trouvée dans IBM ServeRAID Manager

12 février 2020

IBM a émis un avis concernant une vulnérabilité critique référencée CVE-2011-3556 dans son produit ServeRAID Manager, désormais non pris en charge, qui pourrait entraîner l'exécution de code arbitraire.

IBM n'a pas l'intention de publier une mise à jour ou un correctif pour corriger cette vulnérabilité. Au lieu de cela, il est suggéré de configurer ServeRAID Manager pour écouter sur des interfaces réseau spécifiques (comme localhost) ou utiliser un pare-feu basé sur l'hôte pour restreindre l'accès réseau à 34571 / tcp.

Source : http://bit.ly/39PiPOO

Adobe

Vulnérabilité détectée dans Adobe Flash

11 février 2020

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

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

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

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

Actualité

Ransomware exploite le pilote GIGABYTE pour tuer les processus AV

06 février 2020

Les attaquants derrière le RobbinHood Ransomware exploitent un pilote GIGABYTE vulnérable pour installer un pilote malveillant et non signé dans Windows qui est utilisé pour mettre fin au logiciel antivirus et de sécurité.

La plupart des processus de logiciels de sécurité Windows sont protégés contre les arrêts par des processus réguliers et ne peuvent être interrompus que par les pilotes du noyau, qui disposent des autorisations les plus élevées possibles dans Windows. Pour mieux sécuriser Windows, Microsoft a ajouté une stratégie d'application de la signature des pilotes qui empêche l'installation des pilotes du noyau Windows à moins qu'ils n'aient été cosignés par Microsoft. Dans un nouveau rapport, les chercheurs de Sophos ont vu les attaquants RobbinHood installer un pilote GIGABYTE vulnérable connu qui a été cosigné par Microsoft et exploitent sa vulnérabilité pour désactiver la fonction d'application de la signature du pilote de Microsoft.

Une fois désactivée, ils peuvent installer un pilote de noyau malveillant personnalisé qui est utilisé pour mettre fin aux processus antivirus et logiciels de sécurité. Le ransomware sera désormais en mesure de crypter un ordinateur sans crainte d'être détecté. La meilleure façon de vous protéger est de rendre le réseau moins vulnérable.

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

500 extensions Chrome téléchargent secrètement des données privées de millions d'utilisateurs

14 février 2020

Plus de 500 extensions de navigateur téléchargées des millions de fois depuis le Chrome Web Store de Google ont secrètement collecté des données de navigation privées sur des serveurs contrôlés par des attaquants.

Les extensions faisaient partie d'un programme malveillant et de fraude publicitaire de longue date. Des chercheurs de Duo Security, propriété de Cisco, ont finalement identifié 71 extensions du Chrome Web Store qui comptaient plus de 1,7 million d'installations. Après que les chercheurs ont rapporté en privé leurs résultats à Google, la société a identifié plus de 430 extensions supplémentaires. Google a depuis supprimé toutes les extensions connues. […] Alors que chacun des 500 plugins semblait différent, tous contenaient du code source presque identique, à l'exception des noms de fonction, qui étaient uniques. La chercheuse Jamila Kaya a découvert les plugins malveillants à l'aide de CRXcavator , un outil d'évaluation de la sécurité des extensions Chrome.

Un rapport qui contient des détails et une liste de 71 extensions malveillantes, ainsi que leurs domaines associés a été publié. […]

La découverte d'extensions de navigateur plus malveillantes et frauduleuses rappelle que les utilisateurs doivent être prudents lors de l'installation de ces outils et ne les utiliser que lorsqu'ils offrent de véritables avantages.

Source : http://bit.ly/2HtK05v

Vulnérabilité critique dans le réseau LTE

17 février 2020

L'une des normes de sécurité les plus connues dans les télécoms et les réseaux mobiles est l'authentification mutuelle, qui permet à un terminal et à un réseau mobile de vérifier leur identité. Dans la norme Long Term Evolution (LTE), l'authentification mutuelle est définie sur le plan de contrôle, avec une authentification sécurisée et un protocole d'échange de clé.

Récemment, des spécialistes de la sécurité des réseaux dans les universités d'Allemagne et des Émirats arabes unis ont démontré qu'il était possible d'abuser du manque de protection de l'intégrité au niveau-utilisateur pour déployer certaines variantes d'attaques connues sous le nom d'IMPAGT. Les spécialistes de la sécurité réseau ont déployé plusieurs scénarios pour vérifier le comportement des appareils équipés de systèmes d'exploitation iOS ou Android en cas d'une telle attaque.

Pour les opérateurs mobiles, ils s'appuient sur une authentification mutuelle pour facturer ou fournir l'accès à certains sites Web de services qui ne sont accessibles qu'avec un identifiant de couche réseau. Selon les spécialistes de la sécurité des réseaux, les attaques IMP4GT permettent aux acteurs de la menace d'utiliser l'identité des victimes pour accéder à ces services lorsqu'ils ne demandent pas d'autorisation supplémentaire.

Compte tenu de ce qui précède, et parce que la protection de l'intégrité des données des utilisateurs est compatible avec les réseaux 5G, bien qu'elle ne soit pas utilisée dans les cas de double connectivité, **les premières implémentations 5G sont vulnérables à ces attaques.**

Source *: http://bit.ly/2V3UGjk*

Le problème avec les logiciels libres et open source

18 février 2020

Les comptes de développeur non sécurisés, les logiciels hérités et les schémas de nommage non standard sont des problèmes majeurs, conclut l'étude Linux Foundation et Harvard. Une étude de grande envergure menée par des chercheurs de la Linux Foundation et du Laboratory for Innovation Science de Harvard a fourni de nouvelles informations sur les logiciels libres et open source (FOSS) les plus largement utilisés dans les entreprises - et les risques de sécurité potentiels liés à cette utilisation.[…]

Selon les chercheurs, les attaques contre les comptes des développeurs individuels sont en augmentation, et il y a un risque croissant de prises de contrôle de compte et de backdoors et d'autres codes malveillants qui y sont installés et qui peuvent ensuite être utilisés pour accéder au code. Un autre risque lié à l'utilisation répandue des logiciels libres dans les comptes individuels est que les développeurs peuvent décider de supprimer leurs comptes ou de supprimer le code en cas de litiges et de désaccords.

La recherche a montré la nécessité de meilleures conventions de dénomination pour les composants FOSS. Parce que les logiciels libres peuvent être modifiés et copiés librement, […] il est important d'avoir une compréhension commune de l'instance d'un composant FOSS utilisé et de la qualité de sa prise en charge et de sa maintenance. […] Les chercheurs ont également découvert que les anciens composants open source hérités présentent les mêmes risques que les anciennes versions non prises en charge de tout logiciel ou matériel. À titre d'exemple, Le professeur Frank Nagle a souligné la version 0.70 du logiciel PuTTY SSH fréquemment utilisé, qui a été publié en juillet 2017. Aucune mise à jour du logiciel n'a été publiée avant la publication de la version 0.71 près de deux ans plus tard.

Source *: http://bit.ly/3bS8jIb*

Les applications de gestion de documents mobiles populaires mettent les données en péril

02 février 2020

La plupart des applications iOS et Android que Cometdocs a publié sur les magasins d'applications Google et Apple transmettent des documents entiers sans les crypter, ce qui peut potentiellement exposer des données.

L'entreprise de sécurité mobile Wandera, qui a découvert le problème, l'a décrit comme ayant un impact sur 23 des 29 applications Cometdocs sur l'App Store d'Apple […]

Ces applications sont un exemple des risques auxquels les organisations sont confrontées lorsqu'elles permettent aux employés d'utiliser des appareils mobiles non gérés et des applications non approuvées à des fins professionnelles. «Lorsque les utilisateurs introduisent des applications et des configurations informatiques personnalisées sur le lieu de travail sans comprendre comment ils fonctionnent, cela peut causer beaucoup de maux de tête aux professionnels de l'informatique et de la sécurité», explique Covington.

Wandera a déclaré avoir informé Cometdocs à trois reprises entre décembre 2019 et janvier 2020 du problème, mais n'a jusqu'à présent reçu aucune réponse.

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

Linux 5.5 a raté certains correctifs "critiques" du pilote graphique Intel

12 février 2020

Bien que Linux 5.5 soit désormais disponible sur le net en tant que dernière version stable du noyau Linux, il s'avère que certains correctifs du pilote graphique du noyau Intel ont été négligés, ce qui peut causer des problèmes à certains utilisateurs […]. Au moins deux correctifs sont manquants et peuvent conduire Linux 5.5 à fonctionner en système irrécupérable sans aucune possibilité de récupération ou de réinitialisation par les graphiques Intel. Les correctifs doivent encore apparaître dans la file d'attente stable de Linux 5.5, mais il est à espérer qu'ils seront bientôt disponibles et en feront une prochaine version Linux 5.5 points.

Source *: http://bit.ly/37o8Eiz*

Les appareils IoT chez les principaux fabricants infectés par des logiciels malveillants

07 février 2020

Trois des plus grands fabricants mondiaux avaient certains appareils IoT exécutant Windows 7 infectés par un logiciel malveillant dans ce que les experts pensent être une attaque de la chaîne d'approvisionnement.

TrapX Security a rapporté avoir identifié un mineur de crypto-monnaie sur plusieurs appareils IoT chez certains grands fabricants, y compris des véhicules guidés automatiques, une imprimante et une télévision connectée. Les infections ont été détectées en octobre 2019 et les attaquants ont ciblé des systèmes embarqués exécutant Windows 7. Le malware utilisé dans la campagne a été décrit comme un téléchargeur auto-répandu qui exécute des scripts malveillants associés à un mineur de crypto-monnaie nommé Lemon Duck . Le malware a été détecté sur plusieurs véhicules à guidage automatique (AGV). Les AGV sont utilisés pour transporter des matériaux ou effectuer des tâches spécifiques dans une usine de fabrication. Une infection a également été détectée sur un téléviseur intelligent doté d'un PC intégré. Dans un autre exemple, le malware a été repéré sur une imprimante multifonction DesignJet SD Pro, qui avait été utilisée pour imprimer des dessins techniques et qui stockait des données sensibles liées à la gamme de produits de la victime.

Source : *http://bit.ly/38e1zCl*

Les fabricants de périphériques informatiques utilisent des micro-logiciels non signés

19 février 2020

Le fait de ne pas adopter de micro-logiciel signé pour les périphériques informatiques a mis en danger des millions de systèmes Windows et Linux. De nouvelles recherches ont révélé que les micro-logiciels non signés utilisés dans les adaptateurs WiFi, les concentrateurs USB, les trackpads, les caméras pour ordinateurs portables et les cartes d'interface réseau peuvent être utilisés à mauvais escient pour compromettre les ordinateurs et les serveurs.

Ces périphériques sont activement utilisés avec des ordinateurs de Lenovo, HP, Dell et d'autres fabricants. […] Après la divulgation, de nombreux fournisseurs de disques durs et SSD ont apporté des modifications pour s'assurer que leurs composants n'accepteraient que des micro-logiciels valides. Cependant, il y en a beaucoup qui n'ont pas encore suivi la stratégie d'utilisation du firmware signé.

Source : *http://bit.ly/2SR0D1x*

Des défauts critiques affectant des millions de puces HiSilicon

05 février 2020

Vladislav Yarmak, le chercheur russe, a publié un article sur le mécanisme de porte dérobée qu'il a découvert dans les puces HiSilicon, des millions d'appareils intelligents à travers le monde, tels que des caméras de sécurité, des DVR, des NVR et d'autres utilisent ces puces. Le mécanisme de porte dérobée est essentiellement un mélange de quatre anciens bugs de sécurité découverts plus tôt et rendus publics, a déclaré le chercheur en sécurité.

Le chercheur n'a pas signalé le problème à HiSilicon car il ne faisait pas confiance à l'intention du vendeur de le résoudre.

La porte dérobée peut être exploitée en envoyant une série de commandes via le port TCP 9530 aux appareils vulnérables. Les commandes activent le service Telnet sur l'appareil. Une fois le service Telnet opérationnel, l'attaquant peut se connecter avec les identifiants de connexion Telnet trouvés dans les divulgations des années précédentes. Désormais, l'attaquant peut accéder à un compte root qui lui accorde un contrôle total sur l'appareil. Vladislav Yarmak a écrit une preuve de concept (PoC) pour que les utilisateurs testent leur appareil intelligent. Il a aussi fortement suggéré de remplacer immédiatement l'équipement de l'appareil ou bien restreindre complètement l'accès réseau à ces appareils aux utilisateurs de confiance", en particulier sur les ports 23 / tcp, 9530 / tcp, 9527 / tcp - les ports exploitables.

Source : *http://bit.ly/2Sc7u5u* ***PoC :*** *http://bit.ly/3bxKsh4*

Les pirates pourraient éteindre des satellites - ou les transformer en armes

12 février 2020

Amazon, OneWeb et d'autres sociétés tentant de placer des milliers de satellites en orbite dans les mois à venir. Fin janvier, SpaceX comptait 242 satellites en orbite autour de la planète et prévoyait d'en lancer 42 000 au cours de la prochaine décennie […]. Cependant, un danger critique est jusque-là négligé : le manque de normes et de réglementations de cybersécurité pour les satellites commerciaux, aux États-Unis et à l'étranger […]. Si les pirates devaient prendre le contrôle de ces satellites, les conséquences pourraient être désastreuses. Les pirates pourraient simplement éteindre les satellites, empêcher l'accès à leurs services, usurper les signaux des satellites, créant des ravages pour les infrastructures critiques, modifier les orbites des satellites et les écraser sur d'autres satellites ou même sur la Station spatiale internationale. Les fabricants de ces satellites, en particulier les petits CubeSats, utilisent une technologie standard pour maintenir les coûts bas. La grande disponibilité de ces composants signifie que les pirates peuvent les analyser pour détecter les vulnérabilités. De plus, de nombreux composants utilisent la technologie open source. Le danger ici est que les pirates pourraient insérer des portes dérobées et d'autres vulnérabilités dans le logiciel des satellites […].

Étant donné le rythme traditionnellement lent de l'action du Congrès, une approche multipartite impliquant une coopération public-privé peut être justifiée pour garantir les normes de cybersécurité. Quelles que soient les mesures prises par le gouvernement et l'industrie, il est impératif d'agir maintenant.

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

Evènements

Evènements du mois

Bsides Cairo 2020, Egypte

15 Février 2020

http://bit.ly/2TaECd7

Une conférence sur la sécurité de l'information qui a réunie des professionnels du domaine, des chercheurs en sécurité, des universitaires, des étudiants, des entreprises et toute personne qui souhaite partager ses connaissances et apprendre des autres, a eu lieu en Egypte. Les thématiques qui ont été abordées sont : les méthodes de protection des organisations, l'intégration de l'IA à la cybersécurité, des discussions sur les recherches en rapport avec la vulnérabilité buffer overflow et enfin le cloud computing.

Forum régional de l'UIT sur la cybersécurité pour l'Europe et la CEI, Bulgarie

27-28 Février 2020

http://bit.ly/382tdkK

Ce forum est organisé dans le cadre de l'Initiative régionale de l'UIT pour l'Europe sur le renforcement de la confiance dans l'utilisation des TIC et de l'Initiative régionale de l'UIT pour la CEI sur le développement et la réglementation des infrastructures de communication de l'information pour rendre les villes et les établissements humains inclusifs et sûrs, adopté par la Conférence mondiale de développement des télécommunications de l'UIT 2017 (CMDT-17). L'événement a réuni des parties prenantes nationales et internationales dans le domaine de la cybersécurité pour l'échange d'informations sur la confiance et le renforcement de la confiance, la sensibilisation aux risques et la construction de dialogues autour du paysage des cyber-menaces et des pratiques de sécurité actuelles.

Reference	ANPT-2020-BV-02
Titre	Bulletin de veille N°2
Date de version	29 février 2020
Contact	ssi@anpt.dz