BULLETIN DE VEILLE N°6

ANPT-2019-BV-06

« La cyber-sécurité est bien plus qu'une affaire d'informatique.»
- Kirsten Manthorne-

Octobre 2019

Alertes de sécurité

Intel

D'importantes vulnérabilités découvertes dans des processeurs Intel

08 Octobre 2019

De multiples vulnérabilités ont été corrigées dans les produits Intel. Des failles de sécurité critiques dans le micro logiciel du système pour Intel® NUC peuvent permettre à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges. Deux autres vulnérabilités avec une criticité moyenne dans les logiciels Intel® Smart Connect et Intel® Active System Console peuvent permettre à un utilisateur authentifié d'activer l'élévation des privilèges via un accès local.
Il est recommandé de se référer aux bulletins de l'éditeur pour appliquer les correctifs correspondant.

Bulletins *: http://bit.ly/2Wm6E6t ; https://intel.ly/2MY6K16 ; https://intel.ly/2WnwPty*

WhatsApp

Utilisateurs de WhatsApp, il va falloir vous méfier des GIFS animés

04 Octobre 2019

Un chercheur a publié les détails d'une faille d'exécution de code à distance (RCE) sur WhatsApp référencée CVE-2019-11932 qui pourrait être utilisée pour compromettre non seulement l'application, mais également le périphérique mobile sur lequel l'application est exécutée.
La faille exploite un bug permettant de corrompre la mémoire de l'application. L'attaquant envoie une image GIF malveillante par n'importe quel canal ou via WhatsApp. Si WhatsApp est utilisé et que l'attaquant figure dans la liste de contacts de l'utilisateur, ce GIF serait téléchargé automatiquement sur l'appareil et exécuté dès l'ouverture de la galerie WhatsApp.

Les versions d'Android affectées sont *Android 8.1 et Android 9.0.*
Il est recommandé d'appliquer la mise à jour disponible actuellement sur PlayStore.

Source *: http://bit.ly/2WiWRbC*
Exploit *: https://nvd.nist.gov/vuln/detail/CVE-2018-11932*
Détails CVE *: https://nvd.nist.gov/vuln/detail/CVE-2018-11932*

Microsoft

Plusieurs vulnérabilités corrigées dans les produits Microsoft

08 octobre 2019

De multiples vulnérabilités ont été corrigées dans les produits Microsoft. La plus grave d'entre elles est une vulnérabilité d'élévation de privilèges référencée CVE-2019-1378 dans l'Assistant Mise à jour de Windows 10. Un attaquant authentifié localement pourrait exécuter du code arbitraire avec des privilèges système élevés. D'autres vulnérabilités de type divulgation d'information ont été relevées dans le noyau Windows, Hyper-V, le module d'intégrité du code de Windows et le client Windows Update. Un attaquant qui parviendrait à exploiter ces vulnérabilités pourrait accéder aux informations sur le système d'exploitation et le contenu en mémoire.
Les produits affectés sont : Microsoft Windows 10, 8.1, 7 ; Windows Server 2019, 2012, 2008.; Windows Server, version 1903 (Server Core installation).
Il est recommandé de se référer au bulletin de l'éditeur pour plus de détails sur les différentes vulnérabilités et leurs correctifs.

Source *: http://bit.ly/2PoWUa3*

Multiples vulnérabilités dans Microsoft Office

08 Octobre 2019

De multiples vulnérabilités ont été corrigées dans Microsoft Office. Une vulnérabilité dans Microsoft Excel (CVE-2019-1327) permet à un attaquant d'exécuter du code arbitraire dans le contexte de l'utilisateur actuel. Si l'utilisateur actuel est connecté avec des privilèges administrateur, un attaquant

pourrait prendre le contrôle du système affecté. Une vulnérabilité de type élévation des privilèges (CVE-2019-1329) dans SharePoint mène à une autre vulnérabilité (CVE-2019-1328) permet l'usurpation d'identité d'un autre utilisateur du serveur.
Les Ms offices affectés sont : Microsoft Excel 2010 SP2, 2013 et 2016 ; Microsoft Office 2013, 2016 et 2019 ; Office 365 ProPlus.

Il est recommandé de se référer d'appliquer les correctifs détaillés dans le bulletin de l'éditeur.

Source : http://bit.ly/2PoWUa3

Adobe

Mise à jour Adobe corrige plusieurs failles de sécurité

15 Octobre 2019

Une mise à jour massive de sécurité a été publiée pour Experience Manager, Experience Manager Forms, Adobe Acrobat et Reader and Download Manager, couvrant 81 CVE, dont beaucoup sont jugées critiques. Une exploitation réussie pourrait conduire à une exécution de code arbitraire dans le contexte de l'utilisateur actuel et la divulgation d'informations sensibles.
Les systèmes affectés pour les deux plateformes Windows et MacOs sont : Acrobat DC, Acrobat Reader DC, Acrobat 2017 Acrobat Reader 2017, Acrobat 2015, Acrobat Reader 2015.
Il est recommandé aux utilisateurs de mettre à jour leurs installations logicielles avec les dernières versions.

Correctif : https://get.adobe.com/fr/reader/
Source : https://helpx.adobe.com/security/products/acrobat/apsb19-49.html

Android

Multiple vulnérabilités dans l'OS Android

10 octobre 2019

Plusieurs vulnérabilités ont été identifiées dans Android. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités pour provoquer une élévation de privilèges, la divulgation d'informations sensibles et l'exécution de code à distance sur le système ciblé dans le contexte d'un processus privilégié.

Les systèmes affectés sont : Android 7.1.1, 7.1.2, 8.0, 8.1, 9, 10.

Il est recommandé d'appliquer les correctifs publiés par l'éditeur.

Source :https://source.android.com/security/bulletin/2019-10-01.html

Un exploit d'une faille zero-day de la dernière version d'Android

17 Octobre 2019

Une application de preuve de concept fonctionnel (Proof of concept) « *Qu1ckRoot* » a été publiée par un chercheur américain sur github. Cette application peut « rooter » (avoir l'accès super admin) un appareil Android en exploitant une vulnérabilité zero-day (CVE-2019-2215). Cet exploit peut contourner de nombreuses protections de sécurité mises en place au niveau du noyau Android. Seuls les appareils fonctionnant sous Android 8.x et versions ultérieures sont vulnérables.

Les dispositifs affectés sont :

- **Google** : Pixel 1, Pixel 1 XL, Pixel 2, Pixel 2XL;
- **Samsung** : S7, S8, S9;
- **LG** : téléphones Oreo;
- **Motorola** : Moto Z3;
- **Huawei** : P20;
- **Xiaomi** : Redmi Note 5, Redmi 5A, A1;
- **Oppo** : A3.

Il est recommandé d'appliquer les mises à jour nécessaires en se référant au bulletin d'Android du mois d'octobre.

Source : http://bit.ly/2qSAAvp
Bulletin : https://source.android.com/security/bulletin/2019-10-01
Exploit : https://github.com/grant-h/qu1ckr00t

Cisco

Vulnérabilités dans les points d'accès Cisco Aironet

17 Octobre 2019

De multiples vulnérabilités ont été découvertes dans les points d'accès Cisco Aironet. Certaines d'entre elles pourraient permettre à un attaquant distant non authentifié d'obtenir un accès non autorisé à un périphérique ciblé doté de privilèges élevés et provoquer un déni de service, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.
Les systèmes affectés sont :

- Aironet 1540, 1560, 1800, 1810, 1830, 1850, 2800, 3800 Series APs ,4800 APs.
- Catalyst 9100 APs

Il est recommandé d'appliquer les correctifs détaillés sur les bulletins de l'éditeur.

Source : http://bit.ly/2pmX9I3 ; http://bit.ly/31V6jsL ; http://bit.ly/2Wm6E6t

Plusieurs vulnérabilités ont été découvertes dans les produits Cisco

15 Octobre 2019

De multiples vulnérabilités ont été corrigées dans les produits Cisco. La plus grave d'entre elles pourrait permettre l'exécution d'un code arbitraire avec les ***privilèges root*** sur le système affecté. Un attaquant pourrait installer des programmes, afficher, modifier ou supprimer des données, ou encore créer de nouveaux comptes.
Il est recommandé d'installer les mises à jour fournies par l'éditeur.

Source : http://bit.ly/2orIY46

Linux

Multiples vulnérabilités dans le noyau Linux RT de Red Hat

16 Octobre 2019

De multiples vulnérabilités ont été découvertes dans le noyau Linux RT de Red Hat. Une exploitation réussie de ces vulnérabilités permet l'exécution du code arbitraire à distance, un déni de service et une élévation de privilèges.

Les systèmes affectés sont : Red Hat Enterprise Linux 8, 7, 6, 5 et Red Hat Enterprise MRG 2.

Il est à noter que seuls les correctifs pour Red Hat Entreprise 7 et 8 sont disponibles, et que le support étendu de Red Hat Entreprise 5 a pris fin le 31 mars 2017.

Il est recommandé d'utiliser, au minimum, Red Hat Entreprise 7 et d'appliquer les correctifs publiés par l'éditeur.

Source *: https://access.redhat.com/errata/RHSA-2019:3089*

Une vulnérabilité corrigée dans « sudo »

16 Octobre 2019

Une faille de sécurité a été découverte dans « sudo », l'utilitaire utilisé dans de nombreux systèmes Linux/Unix afin de conférer les droits d'accès root à un processus exécuté par un utilisateur aux privilèges moindre. Cette vulnérabilité qui permet une élévation de privilège référencée CVE-2019-14287, autorise un utilisateur à avoir recours à l'utilitaire Sudo sur toutes les commandes du système, en dépit des restrictions inscrites dans le fichier /etc/sudoers. La faille n'était utilisable que sur les systèmes exploitant le fichier /etc/sudoers, qui n'est pas activé par défaut sur l'ensemble des distributions.

Une faille de sécurité assez anecdotique, mais qui pouvait permettre à un programme ou un utilisateur malveillant d'exécuter du code sur la machine avec des privilèges élevés. Et Sudo étant implémenté sur l'ensemble des distributions Linux, la faille mérite d'être corrigée. Heureusement, les développeurs des différentes distributions ne s'y sont pas trompés et les correctifs ont été rapidement diffusées. La version de Sudo implémentant le correctif est la version 1.8.28. Il est recommandé de vérifier la version déployée dans vos distributions linux.

Source *: http://bit.ly/2MXFShK*
Détail CVE *: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14287*

VMware

Vulnérabilité dans les produits VMware

16 octobre 2019

Une vulnérabilité nommée CVE-2019-16919 a été découverte dans les produits VMware. Une exploitation réussie de cette vulnérabilité peut provoquer une élévation de privilèges qui permet à un attaquant de lire et modifier des données.
Les produits affectés sont : VMware Cloud Foundation et Registre de conteneur VMware Harbor pour PCF.

Il est recommandé d'appliquer les correctifs publiés par l'éditeur.

Source *: https://www.vmware.com/security/advisories/VMSA-2019-0016.html*

Oracle

Multiples vulnérabilités dans Oracle Database Server

16 Octobre 2019

De multiples vulnérabilités ont été découvertes dans Oracle Database Server. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à l'intégrité et à la confidentialité des données. Deux de ces vulnérabilités peuvent être exploitées à distance sans authentification, c'est-à-dire qu'elles peuvent être exploitées sur un réseau sans nécessiter d'informations d'identification de l'utilisateur.
Les systèmes affectés sont : Oracle Database Server versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, 19c.

Il est recommandé d'appliquer les correctifs publiés par l'éditeur.

Source *: http://bit.ly/2Jy798h*

PHP

Vulnérabilité dans PHP

29 octobre 2019

Le CERT-FR a publié un avis concernant la vulnérabilité CVE-2019-11043 qui affecte PHP et permet l'exécution de code arbitraire à distance. Un code d'exploitation est maintenant disponible sur internet, facilitant l'utilisation de cette vulnérabilité.
Ce code d'exploitation nécessite une configuration communément recommandée de nginx et php-fpm utilisant fastcgi_split_path_info
Les versions affectées sont : PHP v7.3.x antérieures à 7.3.11 ; PHP v7.2.x antérieures à 7.2.24 ; PHP v7.1.x antérieures à 7.1.33
Les versions de PHP antérieures à 7.1 peuvent être également affectées, et ne bénéficieront pas de mise à jour. Il est primordial d'utiliser une version supportée par l'éditeur.
Il est fortement recommandé de mettre à jour php vers une version non vulnérable et ce dans les plus brefs délais.

Source *: https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-014/*

Actualité

Cybercriminalité : L'Algérie est parmi les pays les plus ciblés

06 octobre 2019

L'Algérie fait partie des pays les plus ciblés en termes d'actes de cybercriminalité. Une information révélée par un rapport de Kaspersky**.** Triste nouvelle pour les internautes algériens, notamment les mobinautes, qui sont les utilisateurs les plus touchés au monde, principalement par des malwares ces deux derniers mois. Ce classement s'explique par l'accès tardif à l'internet mobile en Algérie. Une technologie qui s'installe très bien mais qui reste très jeune d'un point de vue culturel. Notons que l'Algérie est suivie dans ce classement par le Népal et l'Albanie.

Source **:** *https://fibladi.com/news/fr/cybercriminalite-lalgerie-parmi-les-pays-les-plus-cibles/*

L'ARPCE coupe les accès Internet au centre visa VFS Global d'Alger

13 octobre 2019

L'Autorité de Régulation de la Poste et des Communications électroniques (ARPCE) a suspendu les services d'accès à internet au centre VFS Global d'Alger suite à l'exploitation d'un réseau virtuel privé (VPN) en dehors du cadre réglementaire représentant une violation aux dispositions législatives et réglementaires en vigueur.

En effet, un VPN est un dispositif permettant de simuler une adresse IP pour la délocaliser du pays où la connexion internet est établie. Afin d'en exploiter ses services, une autorisation doit être délivrée par l'ARPCE suite à une soumission d'un dossier.

Il est recommandé de se référer au site de l'ARPCE détaillant le dossier à fournir ainsi que le cadre législatif régissant cette activité.

Site : *https://www.arpce.dz/fr*

Des pirates présumés russes modifient Chrome et Firefox pour suivre le trafic Web sécurisé

07 octobre 2019

De nombreux pirates informatiques s'intéressent aux navigateurs internet (Chrome, Edge, Firefox, Opera…) en visant les failles récurrentes dans les outils de navigation sur le web.

Un groupe de malveillants Russe, repéré par Kaspersky et baptisé Turla s'invite dans le trafic Web chiffré TLS en modifiant les certificats installés dans Chrome et Firefox. Les pirates infiltrent d'abord l'ordinateur via un cheval de Troie, ils modifient les certificats d'origines et puis placent leurs propres signatures. Bilan, ils peuvent espionner passivement le trafic chiffré.

Ce groupe est reconnu pour être le groupe de hackers les plus sophistiqués d'aujourd'hui de par les techniques et astuces qu'ils emploient pour compromettre leurs cibles.

Source : *https://www.zataz.com/dissidents-certificats-tls-modifies-des-russes-a-la-manoeuvre/*

Des universitaires découvrent huit vulnérabilités dans les composants VoIP d'Android

02 octobre 2019

Une équipe d'universitaires a découvert huit vulnérabilités dans les composants VoIP du système d'exploitation Android. Ces vulnérabilités peuvent être exploitées pour passer des appels VoIP non autorisés, usurper l'identité de l'appelant, refuser des appels vocaux et même exécuter du code malveillant sur les appareils des utilisateurs.

Au cours des dernières années, ils ont mis au point trois méthodes d'analyse du backend VoIP d'Android. La plupart de leurs tests ont consisté à utiliser du « fuzzing », une technique de test logiciel automatisée bien connue qui permet d'observer son comportement et de rechercher des anomalies dans les résultats ; telles que des crashs ou des fuites de mémoire.

Les travaux de l'équipe de recherche ont permis d'identifier huit vulnérabilités dont plusieurs exploitations ont été développées, on cite « Déni de service à distance sur un appel », « exécution de code à distance en raison d'un buffer overflow », « fuite de données permanente provoquée par un path traversal », « Usurpation d'identité de l'appelant en raison d'une mauvaise analyse du caractère "&" »…etc.

Source : *http://bit.ly/2PqXP9Y*

Sécurité mobile : ces applications de santé ne sont pas bonnes pour votre téléphone ou votre vie privée

08 octobre 2019

Les personnes à la recherche d'informations sur le diabète et d'autres maladies pourraient courir le risque de se voir voler leurs informations personnelles et de voir leur vie privée pillée par les cybercriminels.

La raison pour les pirates de créer des applications malveillantes de santé est qu'elles peuvent facilement être utilisées pour voler des données ou installer d'autres logiciels malveillants - ou les deux - chez un grand nombre de personnes. Une application malveillante prétendra par exemple qu'elle prédira votre espérance de vie si l'utilisateur répond à une liste de questions sur sa santé. Cependant, l'information saisie dans le formulaire sera envoyée à un serveur distant sans que l'utilisateur ne le sache.

Une autre application malveillante fournit des conseils sur le diabète, mais suit également presque tout ce que l'utilisateur fait y compris la position GPS de l'appareil, son adresse IP et les autres applications sur l'appareil, exposant ainsi la vie privée de la victime. Cette application est aussi utilisée pour la difusion de publicités pop-up malveillantes.

Source : *http://bit.ly/34mvl5N*

L'agence allemande de cybersécurité recommande Firefox

18 octobre 2019

Firefox est le seul navigateur à avoir obtenu les meilleures notes lors d'un récent audit effectué par l'agence allemande de sécurité informatique.

L'Office fédéral allemand de la sécurité de l'information (BSI) a testé Mozilla Firefox 68 (ESR), Google Chrome 76, Microsoft Internet Explorer 11 et Microsoft Edge 44. L'audit a été effectué en se basant sur des règles détaillées dans une directive pour les "navigateurs sécurisés modernes" publiée par le BSI le mois dernier (septembre 2019).

Le BSI utilise ce guide pour conseiller les agences gouvernementales et les entreprises du secteur privé sur les navigateurs sûrs à utiliser. L'article comprend une liste de toutes

les exigences minimales requises pour que le BSI considère un navigateur comme "sécurisé". Il répertorie également les domaines dans lesquels les autres navigateurs ont échoué, tels que: Absence de prise en charge d'un mécanisme de mot de passe principal (Chrome, IE, Edge); Aucun mécanisme de mise à jour intégré (IE) et aucune option pour bloquer la collecte de télémétrie (Chrome, IE, Edge).

Source *: http://bit.ly/2Wl0YtA*

15 applications à supprimer sur Android

16 octobre 2019

Les 15 applications concernées ont été téléchargées au total de 1.3 millions de fois depuis janvier dernier, et contiendraient selon les mêmes experts un sous-programme du type adware qui harcèle l'utilisateur avec des publicités intrusives qui peuvent apparaitre à tout moment.
Le plus dangereux dans le mode de fonctionnement de ces applications, c'est qu'elles dissimulent leurs icônes pour empêcher l'utilisateur de les repérer et de les supprimer faisant en sorte que l'utilisateur oublie carrément leur présence sur le téléphone. Le déclanchement des publicités quant à lui ne se fait qu'après quelques heures à partir de l'heure de téléchargement, faisant dissiper le doute sur leur origine, et empêchant ainsi l'utilisateur de les désinstaller depuis le Google Play Store.

Les applications concernées sont: Flash on Calls and Messages, Read QR Code, Image Magic, Generate Elves, Savexpense, QR Artifact, Find your Phone, Scavenger-Speed, Auto Cut Out (Pro et 2019), Background Cut Out, Photo Background, Image Processing. Il est recommandé à toute personne ayant l'une ou plusieurs de ces applications installées sur son téléphone de les désinstaller au plus vite.

Source *: http://bit.ly/34bmnrO*

Avast a révélé une brèche de sécurité ayant affecté son réseau interne

21 octobre 2019

Avast a déclaré que l'attaque avait débuté lorsque l'attaquant avait compromis les informations d'identification VPN d'un employé et obtenu l'accès à un compte qui n'était pas protégé. "L'utilisateur, dont les informations d'identification étaient apparemment compromises et associées à l'adresse IP, ne disposait pas de privilèges d'administrateur de domaine. Toutefois, après une élévation réussie des privilèges, l'attaquant a réussi à obtenir les privilèges d'administrateur de domaine", a déclaré Jaya Baloo, responsable de la sécurité des informations chez Avast.

La société a expliqué qu'elle pensait que le but de cette attaque était d'insérer un logiciel malveillant dans le logiciel CCleaner. L'intrusion a été détectée le 23 septembre, mais Avast avait délibérément laissé le profil VPN compromis actif, dans le but de suivre l'attaquant et d'observer ses actions. Parallèlement, Avast a également modifié le certificat numérique utilisé pour signer les mises à jour de CCleaner. La nouvelle mise à jour a été signée avec un nouveau certificat numérique et la société a révoqué le précédent certificat utilisé pour signer les anciennes versions de CCleaner dans le but d'empêcher les attaquants de signer de fausses mises à jour de CCleaner, au cas où les pirates informatiques parviendraient à mettre la main sur l'ancien certificat.
Cette situation a duré jusqu'au 15 octobre, date à laquelle la société terminait l'audit des versions précédentes de CCleaner et publiait une nouvelle mise à jour saine.

Source *: http://bit.ly/2orP7xc*

Galaxy S10 : Samsung commence à corriger la faille dans le lecteur d'empreintes digitales

24 octobre 2019

Samsung vient d'envoyer une notification qui indique qu'un correctif est en cours de déploiement. Ce correctif intitulé **Biometrics update** doit résoudre le problème causé par le lecteur ultrasonique d'empreintes digitales. Le lecteur peut confondre la texture de certains films protecteurs d'écran avec une empreinte digitale, ce qui permet de déverrouiller le smartphone sans avoir à poser son doigt.

La notification est envoyée uniquement aux utilisateurs qui ont déjà enregistré des empreintes digitales et concerne les Galaxy S10, S10+, Note 10 et Note 10+. Après la mise à jour, Samsung demande aux utilisateurs de supprimer les empreintes enregistrées, puis de les enregistrer à nouveau sans la présence du film protecteur. Le constructeur recommande de ne pas utiliser de film protecteur, en particulier les modèles en silicone avec une surface intérieure texturée perturbant les capteurs d'empreinte.

La mise à jour est pour l'instant uniquement disponible en Corée du sud, mais devrait être rapidement déployée dans les autres pays.

Source *: http://bit.ly/2q5zxrK*

Les piratages et vulnérabilités les plus effrayants de 2019

28 octobre 2019

Un résumé des attaques et menaces sur la sécurité des informations au cours des 10 derniers mois de l'année 2019 a été publié par la plateforme web *zdnet*. Il a été constaté que cette année a été témoin de multiples atteinte à la sécurité des données plus virulente et plus destructives que les années précédentes.

Source *https://www.zdnet.com/article/the-scariest-hacks-and-vulnerabilities-of-2019/*

Evènements

Evènements du mois

Identity Days,

Un évènement unique dédié à la gestion et des accès, et cybersécurité des identités digitales, Paris

24 octobre 2019

En partenariat avec des entreprises prédominantes sur le marché du management de l'identité et des accès (IAM) telles que Microsoft, OneLogin, Alsid et UserCube, la CADIM organise la toute première édition des Identity Days, une journée de conférences articulée autour de quatre thèmes : Cybersécurité des annuaires, Gestion des identités et des méta-annuaires, Gestion des identités dans le Cloud ainsi que Cybersécurité des identités, des privilèges et des accès.

L'événement Identity Days a vocation à permettre aux participants d'échanger autour des différentes perspectives et opportunités offertes par l'IAM et des moyens à mettre en œuvre afin d'intégrer ces nouvelles technologies au sein de la stratégie digitale de l'entreprise.

2eme forum Algero-Britannique de la cybersécurité, FABC 2019, Alger

29 – 30 octobre 2019

La rencontre FABC visait à : DÉCLOISONNER les enjeux de la cybersécurité en réunissant des acteurs de la transformation numérique, les spécialistes de la gestion des risques, les experts en sécurité, les architectes et développeurs, les juristes… ; ACCÉLERER le développement d'un marché européen de la cybersécurité ; FAVORISER l'innovation dans la confiance numérique ; CONSTRUIRE une approche inclusive de la cybersécurité dans la transformation des organisations ; ABORDER la cybersécurité en mixant approche "top down" et "bottom up".

Les Assises de la Sécurité et des Systèmes d'Information, Monaco

09-12 octobre 2019

Les Assises de la Sécurité et des Systèmes d'Information ont tenu leur 19e édition du 9 au 12 octobre à Monaco.

3 jours de forum rythmés par des conférences, rendez-vous, tables rondes, networking et autres ateliers où les professionnels pourront échanger, débattre et discuter des différents enjeux propres à la cyberdéfense. Plusieurs prix ont été attribués notamment le plus grand prix des RSSI, le prix de l'innovation et l'annonce du nouvel évènement « Cybersecuritiy Connect UK » prochainement prévu pour novembre 2019.

Reference	ANPT-2019-BV-06
Titre	Bulletin de veille N°6
Date de version	31 octobre 2019
Contact	ssi@anpt.dz