BULLETIN DE VEILLE N°6

ANPT-2020-BV-06

"Si vous automaltisez un désordre, vous obtenez un désordre automatisé."
- Rod Michael -

Juin 2020

Alertes de sécurité

Microsoft

SMBGhost - Les fantômes des bugs SMB continuent de hanter les chercheurs en sécurité

05 juin 2020

Server Message Block (SMB), le protocole réseau utilisé pour le partage de fichiers et les communications réseau interprocessus, fait l'objet de controverses depuis longtemps, notamment après les attaques de Wannacry et NotPetya.

Récemment, un PoC d'une vulnérabilité critique dans Microsoft Server Message Block (SMB 3.1.1) a été rendu disponible, ce qui pourrait permettre à un attaquant d'exécuter du code à distance sur des machines Windows 10.

Ce code pour l'exploit SMBGhost RCE a été partagé par un chercheur avec pour nom d'utilisateur GitHub 'chompie1337' et a été divulgué publiquement sur Twitter via le pseudo Twitter 'Chompie'. L'exploit repose sur une primitive de lecture physique, qui peut également permettre l'exploitation de futurs bugs de corruption de mémoire SMB.

Microsoft a publié la mise à jour du correctif (KB4551762) pour résoudre ce problème. Microsoft a également fourni plusieurs solutions de contournement, notamment la désactivation de la compression sur les serveurs SMBv3 et le blocage du port TCP 445 (le cas échéant) au niveau du pare-feu périmétrique de l'entreprise.

Source : *https://bit.ly/2ZJ0C9H*

Des mises à jour de Windows 10 ont causé des interruptions d'impression

12 juin 2020

Les utilisateurs de Windows 10 ont signalé qu'ils ne pouvaient pas imprimer à l'aide de périphériques de plusieurs fournisseurs après l'installation des mises à jour pour les périphériques Windows 10 versions 1903, 1909 et 2004, publiées le 9 juin 2020. KB4560960 et KB4557957 , les mises à jour à l'origine de ces problèmes, sont des mises à jour cumulatives avec des correctifs de sécurité pour plusieurs composants Windows 10, ainsi que des améliorations et des correctifs pour diverses fonctionnalités de Windows 10.

Afin de contourner ce désagrément en risquant de compromettre la sécurité de votre système, vous pouvez désinstaller KB4560960 ou KB4557957.

Source : *https://bit.ly/3eh8WMm*

Une faille de la GPO Windows permet aux hackers d'obtenir des privilèges d'administrateur

09 juin 2020

Microsoft a corrigé une vulnérabilité référencée CVE-2020-1317 dans toutes les versions actuelles de Windows. Cette vulnérabilité permet à un attaquant d'exploiter la fonctionnalité de stratégie de groupe Windows pour prendre totalement contrôle d'un ordinateur. Cette vulnérabilité affecte toutes les versions de Windows depuis Windows Server 2008.

Ces stratégies permettent à un administrateur de contrôler la façon dont un ordinateur peut être utilisé, comme la désactivation des paramètres dans les applications, l'interdiction des applications de s'exécuter, l'activation et la désactivation des fonctionnalités Windows, et même le déploiement du même fond d'écran sur chaque ordinateur Windows.

Comme cette vulnérabilité affecte des millions, voire un milliard d'appareils , il s'agit d'une grave faille de sécurité qui devrait être corrigée par tous les administrateurs Windows dès que possible.

Source : *https://bit.ly/3g6bBcl*

FortiGuard Labs a découvert une vulnérabilité d'élévation de privilèges dans Windows 10

11 juin 2020

Une vulnérabilité d'élévation de privilèges liée à la confidentialité des utilisateurs dans Microsoft Windows 10 a été découverte par

FortiGuard Labs. Microsoft a publié un correctif de sécurité pour la vulnérabilités identifiée comme CVE-2020-1296 . La cause principale de cette vulnérabilité est l'absence de séparation des paramètres de confidentialité et la mauvaise gestion des données de diagnostic Windows en mémoire pour tous les utilisateurs Windows 10.

En raison de l'importance de cette vulnérabilité et de ses implications en termes de confidentialité des utilisateurs, nous recommandons aux utilisateurs d'appliquer ces correctifs Microsoft dès que possible.

Plateformes concernées : Windows 10 et Windows Server 2019

Source : *https://bit.ly/3icapps*

Réseaux sociaux

Un bug dans Facebook Messenger pour Windows

11 juin 2020

Les chercheurs en cyber sécurité de Reason Labs, la branche de recherche sur les menaces du fournisseur de solutions de sécurité Reason Cybersecurity , ont dévoilé les détails d'une vulnérabilité récemment découverte dans l'application Facebook Messenger pour Windows.

La vulnérabilité, qui réside dans Messenger version 460.16, pourrait permettre aux attaquants de tirer parti de l'application pour exécuter potentiellement des fichiers malveillants déjà présents sur un système compromis afin d'essayer d'aider les logiciels malveillants à obtenir un accès persistant / étendu.

Selon les chercheurs, l'application vulnérable déclenche un appel pour charger Windows Powershell à partir du chemin *C:\python27*. Les attaquants peuvent pirater ces appels qui tentent de charger des ressources potentiellement inexistantes pour exécuter secrètement des logiciels malveillants. De plus, puisque le répertoire ciblé se trouve également dans un emplacement à faible intégrité, les programmes malveillants pourraient accéder au chemin sans privilèges administrateur.

La vulnérabilité a été corrigée dans la version 480.5, qui est la version la plus récente testée par Reason.

Source : *https://bit.ly/389tgrE*

Cisco

Vulnérabilité de divulgation d'informations dans l'application Cisco Webex Meetings pour Windows

17 juin 2020

Une vulnérabilité dans l'application Cisco Webex Meetings Desktop de Windows pourrait permettre à un attaquant local authentifié d'accéder à des informations sensibles sur un système affecté. Référencée CVE-2020-3347, cette vulnérabilité est due à une utilisation non sécurisée de la mémoire partagée par l'application. Dans un scénario d'attaque, tout utilisateur local ou processus malveillants s'exécutant sur un ordinateur sur lequel WebEx Client pour Windows est installé peut surveiller le fichier mappé en mémoire pour un jeton de connexion. Une fois trouvé, le jeton, comme toutes les informations d'identification divulguées, peut être utilisé pour se connecter au compte Webex en question, télécharger des enregistrements, afficher/modifier des réunions, etc.

Il est recommandé aux utilisateurs de Cisco Webex pour Windows de mettre à niveau vers la version 40.6.0 ou la version la plus récente dès que possible. Toutes les versions antérieures à la version 40.6.0 sont affectées.

Source ; *https://bit.ly/2YzAIy8*

PoC : *https://bit.ly/2NwRLuH*

Zoom

Deux failles critiques dans Zoom

03 juin 2020

Des chercheurs en cyber sécurité de Cisco Talos ont dévoilé avoir découvert deux vulnérabilités critiques dans le logiciel Zoom qui pourrait permettre à des attaquants de pirater à distance les systèmes des participants à un chat de groupe ou d'un destinataire individuel.

Les deux failles en question sont des vulnérabilités de traversée de chemin (path traversal) qui peuvent être exploitées pour écrire ou planter des fichiers arbitraires sur les systèmes exécutant des versions vulnérables du logiciel de vidéoconférence pour exécuter un code malveillant.

La première faille de sécurité (CVE-2020-6109) réside dans la façon dont Zoom exploite le service GIPHY (récemment racheté par Facebook) afin de permettre à ses utilisateurs d'échanger des GIFs lors de discutions. La source de ces GIFs n'est pas vérifiée par l'application ce qui permettrait à un attaquant d'intégrer des GIF provenant d'un serveur tiers contrôlé par celui-ci.

La seconde vulnérabilité d'exécution de code à distance (CVE-2020-6110) réside dans la façon dont les versions vulnérables des extraits de code de processus d'application Zoom étaient partagées via le chat.

Les chercheurs de Cisco Talos ont testé les deux failles de la version 4.6.10 de l'application cliente Zoom et l'ont signalée à l'entreprise. Zoom a corrigé les deux vulnérabilités critiques avec la sortie de la version 4.6.12 de son logiciel Windows, macOS et Linux.

Source : *https://bit.ly/3i5MboC*

Google

Mises à jour de sécurité pour Chrome

23 juin 2020

Google a publié ce mois trois nouvelles versions de Chrome (83.0.4103.97, 83.0.4103.106 et 83.0.4103.116) dans le but de corriger plusieurs vulnérabilités qui pourraient permettre à un attaquant de les exploiter et de prendre le contrôle d'un système affecté.

La dernière version corrige une vulnérabilité qu'un attaquant distant pourrait exploiter pour provoquer une condition de déni de service. CISA encourage les utilisateurs et les administrateurs à consulter la note de version de Chrome et à appliquer les mises à jour nécessaires.

Source : *https://bit.ly/3g6aMjL*

Firefox

Mozilla corrige 5 failles importantes de Firefox

5 juin 2020

Mozilla a publié une mise à jour de Firefox un jour seulement après avoir publié une nouvelle version majeure du navigateur qui a corrigé huit failles de la liste CVE.

L'équipe de Mozilla a publié Firefox 77.0 pour Windows, macOS et Linux. La nouvelle version a été livrée avec un plusieurs nouvelles fonctionnalités et améliorations, ainsi que d'importants correctifs de sécurité. Le lendemain, la version 77.0.1 a été publiée pour toutes les plates-formes de bureau prises en charge, alors que le déploiement de Firefox 77.0 a été interrompu. Cette fois-ci, la mise à jour portait sur un problème concernant l'utilisation du DNS par le navigateur sur HTTPS (DoH), un protocole que le fabricant du navigateur a d'abord activé par défaut pour les utilisateurs basés aux États-Unis il y a un peu plus de trois mois. À moins que vous n'ayez déjà appliqué les dernières mises à jour, vous seriez bien avisé de les vérifier en vous rendant dans le menu du navigateur, puis en cliquant sur Aide et sur À propos de Firefox.

Source : *https://bit.ly/2BIsmeT*

GnuTLS

GnuTLS a corrigé une énorme faille de sécurité vieille de deux ans

10 juin 2020

GnuTLS, une bibliothèque open source largement utilisée mettant en œuvre la sécurité de la couche transport via TLS (Transport Layer Security), a corrigé un bug qui se cachait dans le code depuis près de deux ans, rendant les sessions TLS 1.3 reprises vulnérables aux attaques.

La négociation TLS nécessite deux allers-retours entre le client et le serveur pour établir une connexion sécurisée. Les tickets de session permettent de reprendre les connexions précédemment établies avec un seul aller-retour. Mais cette commodité à un coût - elle est moins sécurisée, comme décrit par le cryptographe Google Filippo Valsorda. La vulnérabilité a été corrigée dans la version dans GnuTLS 3.6.14.

Source : *https://bit.ly/31pzibC*

VMware

Un chercheur de Google découvre une vulnérabilité dans les produits de virtualisation VMware

10 juin 2020

VMware a informé ses clients qu'il avait corrigé une vulnérabilité de divulgation d'informations très grave affectant ses produits de virtualisation Workstation, Fusion et vSphere.
La faille, identifiée comme CVE-2020-3960 , a été signalée à VMware par Cfir Cohen, chercheur de l'équipe de sécurité cloud de Google.
Selon VMware, Cohen a découvert que ESXi, Workstation et Fusion sont affectés par une vulnérabilité de lecture hors limites qui peut permettre à un attaquant disposant d'un accès non administrateur à une machine virtuelle de lire des informations privilégiées de la mémoire.

Le problème affecte ESXi 6.5 et 6.7, Workstation 15.x et Fusion 11.x. Des correctifs ont été publiés, mais aucune solution de contournement ne semble être disponible. VMware a également informé les clients d'une vulnérabilité d'élévation de privilèges affectant Horizon Client pour Windows.

La faille , causée par « la configuration des autorisations de dossier et le chargement non sécurisé des bibliothèques » peut permettre à un attaquant local d'exécuter des commandes comme n'importe quel utilisateur. L'un des chercheurs qui a signalé les failles à VMware, Rich Mirch de Critical Start, a dévoilé les détails du problème le plus récent et a fourni un exploit en preuve de concept (PoC).

Source : *https://bit.ly/388nmMt*

D-Link

6 nouvelles vulnérabilités trouvées sur les routeurs domestiques D-Link

12 juin 2020

Les vulnérabilités référencées CVE-2020-13782 CVE-2020-13786 CVE-2020-13785 CVE-2020-13784 CVE-2020-13783 CVE-2020-13787 ont été trouvées dans le modèle DIR-865L de routeurs D-Link, destiné à un usage domestique. La tendance actuelle au travail à domicile augmente la probabilité d'attaques malveillantes contre les réseaux domestiques, ce qui rend encore plus impérative la mise à jour des périphériques réseau.

Différentes combinaisons de ces vulnérabilités peuvent entraîner des risques importants. Par exemple, des utilisateurs malveillants peuvent renifler le trafic réseau pour voler des cookies de session. Avec ces informations, ils peuvent accéder au portail administratif pour le partage de fichiers, leur donnant la possibilité de charger des fichiers malveillants, de télécharger ou de supprimer des fichiers sensibles. Ils peuvent également utiliser le cookie pour exécuter des commandes arbitraires afin de mener une attaque par déni de service

D-Link a publié un correctif qu'il est fortement recommandé aux consommateurs d'installer, qui peut être trouvé sur le lien suivant : Annonce D-Link

Source : *https://bit.ly/3dDa2AP*

Actualité

Le malware Valak obtient un nouveau plugin pour voler les informations de connexion Outlook

09 juin 2020

Le malware *Valak* a été développé à un rythme accéléré, avec plus de 30 variantes identifiées en six mois. Il a commencé comme un chargeur de logiciels malveillants qui a évolué plus tard vers un voleur d'informations se concentrant sur les cibles de l'entreprise. Il peut infiltrer les serveurs Microsoft Exchange pour voler des données du système de messagerie telles que les informations d'identification et les certificats de domaine qui permettraient d'accéder à un utilisateur de domaine interne.

Dans une analyse technique, des chercheurs de la société de cybersécurité SentinelOne fournissent des détails sur un nouveau plugin appelé «clientgrabber», dont la tâche consiste à voler les informations d'identification de courrier électronique dans le registre d'une machine compromise. L'accès aux boîtes de réception Outlook des utilisateurs permet aux acteurs de la menace d'exécuter ce que l'on appelle des «attaques par chaîne de réponse», où ils introduisent un message malveillant dans un fil de messagerie pour diffuser des logiciels malveillants.

Cette tactique a été observée avec d'autres familles de logiciels malveillants. Emotet a commencé à l'utiliser lors de sa relance l'année dernière et la société indépendante de services de cybersécurité CSIS a repéré QakBot faire de même cette année.

Les chercheurs de Cybereason Nocturnus ont publié fin mai un rapport technique complet sur Valak, détaillant ses techniques, ses composants, ainsi que les principales régions ciblées (États-Unis et Allemagne).

Source : *https://bit.ly/2Nysiko*

Les applications Android peuvent être piratées en exploitant ses composants de messagerie interne

17 juin 2020

Les utilisateurs d'Android sont souvent confrontés à des risques de cybersécurité en raison de vulnérabilités dans les composants internes des applications populaires. Récemment, une de ces vulnérabilités a été identifiée dans le composant interne appelé «Intents». Les chercheurs ont pu démontrer qu'une application Android peut être piratée en invoquant ses composants d'activité exposés en utilisant «Intent».

En juin 2020, les chercheurs ont pu pirater les données sensibles des applications Android via les objets de communication inter-processus d'Android appelés `` Intent ".

Des informations détaillées sur toute application Android (y compris les intentions déclarées) peuvent être obtenues via le fichier AndroidManifest.xml(un fichier manifeste d'application). Avec cela, un attaquant peut obtenir des informations sur la série d'activités exportées se produisant dans l'application.

Après avoir pris connaissance des activités exportées, il est possible d'envoyer une « intention » aux composants « activité » exposés (en utilisant un shell ADB racine), ce qui contournerait les exigences d'authentification, conduisant ainsi à des attaques de contournement d'authentification.

Source : *https://bit.ly/386G3QV*

Faux journaux d'erreurs Windows utilisés pour masquer la charge utile malveillante

25 juin 2020

Les cybercriminels continuent à mettre au point de nouvelles techniques pour éviter leur détection. Récemment, des pirates ont été découverts utilisant de faux journaux d'erreurs pour stocker des caractères ASCII déguisés en valeurs hexadécimales qui décodent en une charge utile malveillante conçue pour préparer le terrain pour des attaques basées sur des scripts.

Pour développer et exécuter leur technique, les auteurs de logiciels malveillants ont cette fois utilisée de nouvelles astuces liées aux journaux d'erreurs pour cacher en pleine vue une nouvelle attaque sophistiquée.

Récemment, les chercheurs de Huntress Labs ont découvert l'attaque qui comprenait des astuces telles que renommer des fichiers légitimes, se faire passer pour une tâche planifiée existante et utiliser une charge utile malveillante stockée dans un fichier conçu pour ressembler à un journal des erreurs à masquer à la vue.

Les fichiers journaux d'erreurs contenaient des horodatages et des références à OS 6.2, le numéro de version interne de Windows pour Windows 8 et Windows Server 2012. La charge utile finale est utilisée pour collecter des détails sur l'hôte compromis, les applications installées, en particulier les logiciels PoS, les applications financières, les navigateurs, les logiciels fiscaux (Lacerte et ProSeries), les produits de sécurité (Kaspersky, Comodo, Defender), les adresses IP, les privilèges administratifs, etc.

Les utilisateurs doivent appliquer les correctifs des vulnérabilités, protéger également les réseaux contre les exploits d'applications, les logiciels malveillants, les botnets et les vulnérabilités zero-day.

Source : *https://bit.ly/31rjWTM*

Un nouveau malware macOS se propage dans les résultats de recherche Google

22 juin 2020

Un nouveau malware a été détecté dans les résultats de Google incitant les utilisateurs à contourner les mesures de sécurité d'Apple pour l'installer. Intego a découvert un nouveau cheval de Troie qui est spécifiquement conçu pour contourner les mesures de sécurité de macOS Catalina.

MacOS Catalina a un certain nombre de précautions pour empêcher l'installation de logiciels malveillants, notamment la

vérification que les développeurs d'applications sont enregistrés auprès d'Apple et s'ils ne préviennent pas les utilisateurs et rendent l'installation du programme plus difficile. Il est possible d'installer un tel programme mais il est nécessaire de faire des changements dans les paramètres système pour ce faire. Ce cheval de Troie particulier est capable de contourner ces restrictions de sécurité car il lance un guide d'installation qui guide l'utilisateur à travers les étapes nécessaires à son installation. Ce cheval de Troie récemment découvert est particulièrement dangereux car il peut être trouvé via les pages de résultats de recherche de Google, rapporte AppleInsider.

La protection la plus simple contre les logiciels malveillants consiste à installer uniquement des logiciels directement à partir du site Web du fabricant. Cependant, la meilleure pratique est de ne pas utiliser Flash Player du tout. Veuillez consultez aussi cette liste de virus Mac.

Source : *https://bit.ly/38818dt*

80 000 imprimantes ont exposé leur port IPP en ligne

23 juin 2020

Pendant des années, les chercheurs en sécurité ont averti que chaque appareil exposé en ligne sans être protégé par un pare-feu est une surface d'attaque. Les pirates peuvent déployer des exploits pour prendre le contrôle d'un appareil, ou ils peuvent simplement se connecter au port exposé si aucune authentification n'est requise. Les appareils piratés de cette manière sont souvent asservis dans des réseaux de zombies malveillants, ou ils servent de premiers points d'ancrage et de portes dérobées à de plus grands réseaux d'entreprise (les pirates russes utilisent déjà cette technique).

Dans un rapport publié plus tôt ce mois-ci , des chercheurs en sécurité de la Shadowserver Foundation, une organisation à but non lucratif axée sur l'amélioration des pratiques de cybersécurité à travers le monde, ont publié un avertissement concernant les entreprises qui laissent les imprimantes exposées en ligne. Plus spécifiquement, les experts de Shadowserver ont scanné les quatre milliards d'adresses IPv4 routables pour les imprimantes qui exposent leur port IPP.

Pour configurer les fonctions de contrôle d'accès IPP et d'authentification IPP, il est conseillé aux utilisateurs de consulter les manuels de leurs imprimantes.

Source : *https://zd.net/3eGMIDF*

Le ver de Golang a élargi sa portée à Windows et a ajouté une capacité de porte dérobée

25 juin 2020

Une nouvelle version d'une campagne de malware connue qui vise à installer des cryptomineurs a changé ses tactiques, ajoutant des attaques sur les serveurs Windows et un nouveau pool d'exploits à son sac de trucs. Il évolue également rapidement pour se positionner comme une porte dérobée pour le téléchargement de futurs logiciels malveillants plus dommageables, selon les chercheurs.

Selon une analyse de Barracuda Networks, le chargeur jusqu'ici sans nom, qu'il appelle désormais «Golang», ne ciblait à l'origine que les machines Linux, mais s'est maintenant propagé à Windows et à d'autres serveurs. Une fois que le logiciel malveillant infecte une machine, il télécharge un ensemble de fichiers personnalisés en fonction de la plate-forme qu'il attaque.

Source : *https://bit.ly/31rkFnY*

La fausse application de suivi des contacts COVID-19 du gouvernement a diffusé un ransomware Android

24 juin 2020

Les gouvernements du monde entier ont pris des mesures pour lutter contre le coronavirus . L'une des tactiques impliquées consiste à utiliser des applications de suivi des contacts pour aider à retrouver les personnes qui ont pu être en contact avec une victime du virus, ce qui les expose elles-mêmes à un risque.

Un de ces pays se trouve être le Canada qui a récemment annoncé la sortie d'une application nommée «COVID Alert» qui sera disponible pour les Canadiens dans tout le pays dans un peu plus d'un mois. Cependant, les attaquants n'ont pas attendu et ont déjà commencé une campagne d'usurpation d'identité en lançant une fausse application Android qui prétend provenir de Santé Canada, mais en réalité, il s'agit d'un malware malveillant qui mène à une infection par un rançongiciel.

Comme l'ont découvert des chercheurs d'ESET, les attaquants proposaient l'APK de l'application via deux noms de domaine, à savoir *tracershield [.] Ca* et *covid19tracer [.] Ca*, qui n'est pas tous deux actifs actuellement. La campagne fonctionne de telle manière qu'une fois que l'utilisateur a installé l'application, elle entraîne l'installation d'un ransomware nommé CryCryptor sur leurs appareils. Le logiciel malveillant demande ensuite des autorisations d'accès aux fichiers sur l'appareil, après quoi il commence ensuite à crypter les données impliquant différentes extensions de fichier […].

Il est conseillé aux utilisateurs d'éviter de faire des téléchargements à partir de magasins d'applications tiers et même d'évaluer soigneusement les applications dans le Google Play Store avant de les télécharger. Installez également un logiciel antivirus fiable et analysez régulièrement votre appareil.

Source : *https://bit.ly/2NzHBsW*

Twitter dit que les utilisateurs professionnels étaient vulnérables à la violation de données

23 juin 2020

Twitter présente ses excuses aux utilisateurs professionnels pour une violation de données tout en annonçant que leurs informations personnelles identifiables pourraient avoir été compromises.

Il s'avère que des détails tels que les adresses e-mail, les numéros de téléphone et les quatre derniers chiffres des numéros de carte de crédit ont été stockés dans les caches de navigateur de ces

utilisateurs. Par conséquent, d'autres personnes utilisant le même ordinateur auraient pu consulter les informations sans autorisation ni authentification supplémentaires.

Twitter a déclaré avoir pris connaissance du problème le 20 mai et a rapidement corrigé la vulnérabilité, mais a jugé nécessaire d'alerter et de présenter des excuses aux utilisateurs professionnels. Il n'a pas révélé le nombre de clients susceptibles d'avoir été affectés par la vulnérabilité. Lisez plus ici .

Source : *https://bit.ly/3g6eOIV*

Evènements

Evènements du mois

Africa Cyber Security Culture Conference

11 juin 2020, en ligne

https://bit.ly/3g2BD07

La Conférence sur la culture de la cybersécurité en Afrique, a eu lieu le 11 juin 2020, des experts de l'industrie de toute l'Afrique se sont réunis pour discuter des principales tendances et sujets liés à la cybersécurité sur le continent. L'événement en ligne d'une demi-journée a accueilli un éventail impressionnant de conférenciers et de panélistes de certaines des marques les plus éminentes du continent et a fourni aux participants des plats à emporter pratiques et proactifs qu'ils pourront mettre en œuvre dans leur organisation.

FranSec: French Virtual IT Security Conference

24-25 juin 2020, Online

https://bit.ly/2BQDZ39

Alors que la numérisation continue de s'accélérer et que les machines deviennent encore plus connectées, la continuité des activités, les revenus et la réputation sont en jeu, ce qui rend vital pour les leaders de l'industrie de placer la cybersécurité au cœur de leur stratégie opérationnelle.

La conférence virtuelle sur la cybersécurité #FranSec, a eu lieu le 24 et 25 juin 2020. Des chefs de file de la cybersécurité ont été réunis pour échanger des connaissances et une expertise approfondie en vue de protéger les principales industries du pays. Cela comprend les principaux acteurs des secteurs bancaire et financier, de l'énergie, des produits de grande consommation, de l'agriculture, des soins de santé, de la fabrication, des transports, etc.

Africa Women in Cyber & Information Security webinar

25 et 26 juin 2020

https://bit.ly/2YFaCde

La conférence inaugurale Africa Women in Cyber & Information Security est un événement de réseautage qui vise à mettre en évidence et à célébrer la valeur et les succès des femmes dans l'industrie de la cybersécurité. L'événement a rassemblé des femmes du secteur privé, du monde universitaire et du gouvernement de toute la région à différents niveaux de carrière. C'est une opportunité pour les femmes passionnées par la cybersécurité de se connecter les unes aux autres, de renforcer les relations et d'en créer de nouvelles.

Reference	ANPT-2020-BV-06
Titre	Bulletin de veille N°6
Date de version	30 Juin 2020
Contact	ssi@anpt.dz