# BULLETIN DE VEILLE N°5

ANPT-2020-BV-05

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

Mai 2020

# Alertes de sécurité

## Microsoft

### Vulnérabilité affectant les serveurs DNS Windows

15 mai 2020

Microsoft a publié un avis d'une vulnérabilité impliquant une amplification de paquets qui affecte les serveurs DNS Windows. Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait entraîner la non-réponse du service Serveur DNS. Pour exploiter cette vulnérabilité, un attaquant devrait avoir accès à au moins un client et un domaine qui répond avec un grand volume d'enregistrements de référence, sans enregistrements de liaison, qui pointent vers des sous-domaines de victimes externes. Lors de la résolution d'un nom du client attaquant, pour chaque enregistrement de référence trouvé, le résolveur contacte le domaine victime. Cette action peut générer un grand nombre de communications entre le résolveur récursif et le serveur DNS faisant autorité de la victime pour provoquer une attaque par déni de service distribué (DDoS).

Aucune mise à jour n'est disponible pour le moment. Cependant, Microsoft recommande de limiter le taux de réponses du serveur DNS.

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

### Mettre à jour Windows pour corriger une faille facilement exploitable

15 mai 2020

Parmi les vulnérabilités corrigées par Microsoft dans son Tuesday patch du mardi 2020 figure la vulnérabilité CVE-2020-1048 d'une sévérité «modérée» et de type élévation de privilèges dans le service Windows Print Spooler. Cette vulnérabilité, qui affecte Windows 7, 8.1 et 10 et Windows Server 2008, 2012, 2016 et 2019, provient du service du spouleur d'impression Windows qui permet l'écriture incorrecte et arbitraire dans le système de fichiers.

La vulnérabilité n'est pas exploitable à distance - un attaquant doit déjà avoir accès au système cible (être connecté) pour pouvoir exécuter un script ou une application spécialement conçue qui exploitera la faille.

Des chercheurs ont partagé plus de détails techniques sur la CVE-2020-1048 et ont expliqué comment est-il possible de l'exploiter pour élever les privilèges, contourner les règles EDR, gagner en persistance, …etc. Ils ont également publié le code d'exploitation PoC et ont surnommé la faille «PrintDemon».

Il est fortement conseillé d'implémenter le correctif dès que possible car, selon les chercheurs, la faille est facile à exploiter avec une seule commande PowerShell.

***Source***: *https://bit.ly/2ZK1V26*

### Microsoft May 2020 Patch Tuesday corrige 111 vulnérabilités

12 mai 2020

Microsoft a corrigé 111 vulnérabilités sur 12 produits différents permettant l'exécution de code à distance, la fuite d'informations, l'élévation de privilèges, le déni de service, l'usurpation d'identité et le contournement de dispositifs de sécurité. Parmi les vulnérabilités nous citons :

CVE-2020-1118 - Une vulnérabilité dans l'implémentation de Windows de Transport Layer Security (TLS) qui pourrait permettre à un attaquant distant non authentifié de redémarrer en continu le système cible, entraînant un déni de service.

CVE-2020-1135 - Une vulnérabilité dans le composant graphique Windows qui pourrait permettre aux attaquants d'élever leurs privilèges sur un système compromis et d'entreprendre des actions comme voler des informations d'identification, installer des logiciels malveillants, etc. La vulnérabilité se trouve dans la plupart des versions de Windows 10 et Windows Server et Microsoft le juge "plus susceptible d'être exploité".

Des informations supplémentaires sur le Patch Tuesday de ce mois sont disponible ici.

Il est recommandé d'appliquer les correctifs de sécurité proposés par Microsoft.

***Source :*** *https://zd.net/2ZNU8QW*

## Android

### Une nouvelle faille Android StrandHogg 2.0 affectant plus d'un milliard de téléphones

26 mai 2020

Des chercheurs de Promon ont découvert une nouvelle vulnérabilité d'élévation de privilèges dans Android qui permet aux pirates d'accéder à presque toutes les applications. La vulnérabilité référencée CVE-2020-0096 a été nommée StrandHogg 2.0 par Promon en raison de ses similitudes avec la fameuse vulnérabilité StrandHogg découverte par la société en 2019. En exploitant cette vulnérabilité, une application malveillante installée sur un appareil peut attaquer et tromper l'utilisateur de sorte que lorsque l'icône de l'application d'une application légitime est cliquée, une version malveillante s'affiche à la place sur l'écran de l'utilisateur.

À l'aide de StrandHogg 2.0, les attaquants peuvent, une fois qu'une application malveillante est installée sur l'appareil, accéder à des SMS et des photos privées, voler les informations d'identification des victimes, suivre les mouvements GPS, établir et / ou enregistrer des conversations téléphoniques et espionner via la caméra d'un téléphone et microphone. Les exploits de StrandHogg 2.0 n'affectent pas les appareils exécutant Android 10. Cependant, avec une proportion importante d'utilisateurs d'Android signalant toujours utiliser des versions plus anciennes du système d'exploitation, un pourcentage important de la population mondiale est toujours à risque. Google a déployé un correctif auprès des partenaires de l'écosystème Android en avril 2020, avec un correctif de sécurité fixe (versions Android 8.0, 8.1 et 9) qui devrait être déployé auprès du grand public en mai 2020.

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

## Intel

### Les failles de Thunderbolt exposent des millions de PC à un piratage manuel

10 mai 2020

Un chercheur en sécurité a découvert une vulnérabilité Thunderbolt qui pourrait permettre aux attaquants de contourner les défenses du système et d'accéder au contenu du lecteur d'un ordinateur verrouillé en quelques minutes - avec des installations Boot Camp de Windows et de Linux sensibles à l'attaque.

Développé et maintenu par Intel, Thunderbolt est une norme de port courante que l'on trouve dans des millions de PC grand public et qui sont compatibles avec Windows, Linux ainsi que Mac Apple. Cependant, certaines fonctionnalités de l'interface Thunderbolt suscitent des inquiétudes chez les experts en sécurité depuis des années.

Bjorn Ruytenberg, chercheur en sécurité à l'Université de Technologie d'Eindhoven, a publié des détails sur une nouvelle vulnérabilité qu'il surnomme "Thunderspy". Avec seulement quelques minutes d'accès physique et quelques centaines de dollars d'équipements faciles à se procurer, la vulnérabilité pourrait permettre à un attaquant de contourner les mécanismes de sécurité d'un ordinateur - même s'il est verrouillé et que son disque dur est crypté.

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

## OpenSSL

### Un PoC a été publié pour la vulnérabilité DoS CVE-2020-1967 dans Openssl

06 mai 2020

Une preuve de concept (PoC) d'un exploit, ainsi que des détails techniques décrivant son processus, a été publiée pour une faille récemment corrigée dans OpenSSL qui permet à un attaquant distant de provoquer des dénis de service (DoS).

La vulnérabilité, référencée CVE-2020-1967 affecte les versions OpenSSL 1.1.1d, 1.1.1e et 1.1.1f, mais n'affecte pas les anciennes versions 1.0.2 et 1.1.0. La faille est décrite comme une erreur de déréférencement du pointeur NULL dans la fonction SSL_check_chain() pendant ou après le handshake du protocole TLS 1.3, et peut être exploitée pour provoquer un déni de service en envoyant un algorithme de signature non valide ou non reconnu.

Le chercheur a déclaré que le processus d'exploitation est assez simple : il suffit d'envoyer la charge utile malveillante au serveur vulnérable en utilisant, par exemple, l'utilitaire patch openssl s_client disponible sur GitHub. La vulnérabilité peut également être exploitée via une attaque man-in-the-middle (MitM) ou en configurant un serveur TLS malveillant et en incitant un client vulnérable à s'y connecter.

Le bug a été corrigé le 21 avril avec la sortie d'OpenSSL 1.1.1g.

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

## Apache

### Une vulnérabilité d'exécution de code à distance dans Apache Tomcat

11 mai 2020

Apache Tomcat a publié un avis sur une vulnérabilité d'exécution de code à distance référencée CVE-2020-9484. Un attaquant peut contrôler le contenu et le nom d'un fichier sur le serveur. L'exploitation de cette vulnérabilité est cependant soumise à de nombreuses conditions.

Les versions affectées :

- Apache Tomcat 10.x < 10.0.0-M5
- Apache Tomcat 9.x < 9.0.35
- Apache Tomcat 8.x < 8.5.55
- Apache Tomcat 7.x < 7.0.104

Il est recommandé aux utilisateurs concernés de mettre Tomcat à niveau vers une version non vulnérable dès que possible. Les utilisateurs qui ne souhaitent pas semettre à niveau peuvent également désactiver temporairement la fonction FileStore ou

configurer la valeur de sessionAttributeValueClassNameFilte séparément pour garantir que seuls les objets avec des attributs spécifiques peuvent être sérialisés / désérialisés.

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

## Bluetooth

### La plupart des appareils Bluetooth sont vulnérables aux attaques d'usurpation d'identité

21 mai 2020

Des vulnérabilités dans le processus d'authentification Bluetooth donnent aux attaquants un moyen d'insérer des appareils malveillants entre deux appareils appariés en toute sécurité, selon des chercheurs universitaires.

La plupart des appareils Bluetooth standard sont vulnérables à ce problème selon les chercheurs, qui ont testé avec succès une attaque de preuve de concept. Celle-ci a été testée sur 31 appareils Bluetooth issus des principaux fournisseurs de matériel et de logiciels. Les puces Bluetooth d'Apple, d'Intel, de Qualcomm, de Cypress, de Broadcomm et d'autres sont toutes vulnérables aux attaques. Les chercheurs affirment que les attaques par usurpation d'identité Bluetooth sont possibles en raison de vulnérabilités dans la norme, notamment l'absence d'un mécanisme d'authentification mutuelle obligatoire.

Cependant, comme un attaquant devrait être physiquement proche d'une cible et avoir besoin de certaines informations sur celle-ci, la probabilité d'attaques massives ou aléatoires est faible, selon certains experts en sécurité.

***Rapport technique :*** *https://bit.ly/3goyVTJ*

***Source :*** *https://bit.ly/3emd7q2*

## Bind

### Les versions de sécurité de BIND 9 corrigent deux vulnérabilités de gravité élevée

20 mai 2020

L'Internet Systems Consortium (ISC) a publié une série de mises à jour sécuritaires qui corrigent les vulnérabilités récemment découvertes dans BIND 9, le logiciel serveur DNS ( Domain Name System ) le plus largement utilisé .

Les deux vulnérabilités - CVE 2020-8616 et CVE 2020-8617 - sont toutes deux de gravité élevée. CVE-2020-8616 se rapporte à la découverte que BIND ne limitait pas suffisamment le nombre de récupérations effectuées lors du traitement des références. La seconde vulnérabilité, CVE-2020-8617, est liée à une erreur logique dans le code BIND 9 qui vérifie la validité de la signature de transaction. La faille pourrait être utilisée pour déclencher un échec d'assertion qui entraînerait un déni de service aux clients.

Il est recommandé aux opérateurs de les corriger « dès que possible ». Les mises à jour sont disponible ici.

***Source :*** *https://bit.ly/36wUmgx*

# Actualité

### Site web du ministère algérien de la santé : Piratage informatique ou simple bug ?

28 mai 2020


Le site web du ministère de la santé de la population et de la réforme hospitalière www.sante.gov.dz a été piraté par un hacker d'origine marocaine surnommé « ox souhail », travaillant avec le groupe « Morrocan Revolution », un groupe de pirates qui exerce de manière malveillante depuis quelques années déjà.

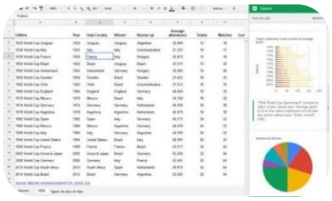
En effet, une récente attaque provenant du Maroc a eu lieu ce Lundi, visant à pirater le site web du ministère algérien de la santé.

Les autorités concernées n'ont pas encore partagé de communiqué au sujet de ce piratage, ciblant l'un des sites web les plus sensibles et les plus visités durant cette crise causée par le COVID-19 qui touche le pays et le monde entier.

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

### Microsoft : Méfiez-vous de cette campagne de phishing massive utilisant des macros Excel malveillantes pour pirater les PC

22 mai 2020



L'équipe Security Intelligence de Microsoft a averti qu'elle suivait une campagne de phishing "massive" qui tente d'installer un outil d'accès à distance sur les PC en incitant les utilisateurs à ouvrir des pièces jointes contenant des macros Excel 4.0 malveillantes.

Microsoft a déclaré que la campagne sur le thème COVID-19 a commencé le 12 mai et continue jusqu'à présent d'envoyer plusieurs centaines de pièces jointes.

Les courriels envoyés prétendent provenir du Centre Johns Hopkins et porter le titre "RAPPORT DE SITUATION COVID-19 DE L'OMS". Si le destinataire tente d'ouvrir les fichiers Excel joints, il s'ouvrira avec un avertissement de sécurité et affichera un graphique des cas supposés de coronavirus aux États-Unis. Mais si elle est autorisée à s'exécuter, la macro Excel 4.0 malveillante télécharge et exécute également NetSupport Manager.

Bien que NetSupport Manager soit un outil d'accès à distance légitime, il est connu pour être utilisé abusivement par des attaquants pour accéder à distance à - et exécuter des

commandes sur - des machines compromises, a déclaré Microsoft. Il se connecte à un serveur de commande et de contrôle (C&C), permettant aux attaquants d'envoyer d'autres commandes.

Ce n'est pas la seule nouvelle menace que l'équipe de sécurité de Microsoft a repéré : elle a également mis en garde contre une nouvelle campagne Trickbot , lancée le 18 mai, qui utilise des courriels prétendant offrir un "contrôle personnel du coronavirus" - une variante du "test COVID-19 gratuit" vu dans les précédents éditions de spam Trickbot. Ce dernier reste l'une des charges utiles les plus courantes dans les campagnes sur le thème COVID-19.

***Source :*** *https://zd.net/2U4MsGz*

## Des milliers de systèmes d'entreprise infectés par le nouveau gang de malwares Blue Mockingbird

25 mai 2020


Des milliers de systèmes d'entreprise auraient été infectés par un logiciel malveillant d'extraction de crypto-monnaie exploité par un groupe suivi sous le nom de code de Blue Mockingbird.

Les chercheurs disent que Blue Mockingbird attaque les serveurs publics exécutant des applications ASP.NET qui utilisent le framework Telerik pour leur composant d'interface utilisateur (UI).

Les pirates informatiques exploitent la vulnérabilité CVE-2019-18935 pour planter un shell Web sur le serveur attaqué. Ils utilisent ensuite une version de la technique Juicy Potato pour obtenir un accès de niveau administrateur et modifier les paramètres du serveur pour obtenir un accès persistant.

Une fois qu'ils ont un accès complet à un système, ils téléchargent et installent une version de XMRRig, une application d'exploration de crypto-monnaie populaire pour la crypto-monnaie Monero (XMR). Les experts de Red Canary disent que si les serveurs IIS accessibles au public sont connectés au réseau interne d'une entreprise, le groupe tente également de se propager en interne via des connexions RDP (Remote Desktop Protocol) ou SMB (Server Message Block) faiblement sécurisée. Dans un avis publié fin avril, la National Security Agency (NSA) des États-Unis a répertorié la vulnérabilité Telerik UI CVE-2019-18935 comme étant l'une des vulnérabilités les plus exploitées, elles sont utilisées pour planter des coquilles Web sur des serveurs. Les entreprises doivent appliquer les correctifs à cette vulnérabilité, et peuvent aussi bloquer les tentatives d'exploitation de la CVE-2019-18935 au niveau de leur pare-feu. En cas d'absence de pare-feu Web, les entreprises doivent rechercher des signes de compromis au niveau du serveur et du poste de travail. Red Canary a publié un rapport avec des indicateurs de compromis pour analyser les serveurs et les systèmes à la recherche de signes d'une attaque Blue Mockingbird.

***Source :*** *https://zd.net/3d5QCoZ*

## Nouveau jailbreak Unc0ver publié, fonctionne sur toutes les versions récentes d'iOS

26 mai 2020


Les jailbreaks sont un type de logiciel personnalisé qui fonctionne en exploitant les bogues du système d'exploitation iOS afin d'accorder aux utilisateurs un accès root et un contrôle total sur leur appareil. Par défaut, Apple ne permet pas aux utilisateurs d'avoir un contrôle total sur leurs iPhones et autres appareils iOS, pour des raisons de sécurité. L'équipe Unc0ver a publié Unc0ver 5.0.0, la dernière version de leur logiciel de jailbreak, qui peut rooter et déverrouiller tous les appareils iOS, même ceux qui exécutent la version iOS la plus récente - iOS v13.5.

Cela est possible, ont-ils déclaré, car Unc0ver 5.0.0 utilise une vulnérabilité zero-day dans le système d'exploitation iOS, une vulnérabilité qu'Apple ne connaît pas.

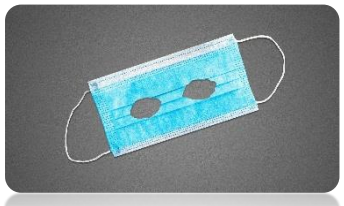
L'équipe Unc0ver a déclaré avoir testé le jailbreak sur iOS 11 à iOS 13.5. Le jailbreak n'a pas fonctionné sur les versions iOS 12.3 à 12.3.2 et 12.4.2 à 12.4.5.

Les experts en sécurité déconseillent généralement de jailbreaker un appareil iOS, car cela ouvre l'appareil aux logiciels malveillants et autres attaques. Apple devrait déployer une mise à jour de sécurité dans les prochains jours pour corriger la vulnérabilité zero-day exploitée par le jailbreak Unc0ver.

***Source :*** *https://zd.net/2X3wo9z*

## Pirates informatiques et espionnage médical

27 mai 2020



Une vague de cyberespionnage autour de la recherche médicale COVID-19 démontre une fois de plus les dangers de traiter la cybersécurité comme un domaine séparé et clos. Des responsables américains ont récemment annoncé une augmentation du nombre de pirates informatiques affiliés au gouvernement chinois ciblant la recherche médicale et d'autres installations aux États-Unis pour obtenir des données sur un éventuel vaccin au COVID-19 ou des traitements efficaces pour lutter contre le virus […].

Pendant des années, les décideurs et les médias ont rangé les menaces et les conflits liés à la cybersécurité dans leur propre silo spécialisé. Mais le monde du cyberespionnage n'est en réalité pas séparé du tout : c'est juste un autre moyen pour les pays de poursuivre leurs objectifs tactiques et stratégiques […].

La pandémie a provoqué une tendance déjà accélérée vers la virtualisation de notre travail et de nos vies privées. Ce qui est vrai pour nous en tant qu'individus vaut également pour les États : ils espionnent plus en ligne parce que la vie se déroule en ligne […].

***Source :*** *https://bit.ly/2AcwDq8*

## Avez-vous corrigé ces 10 vulnérabilités les plus fréquemment exploitées ?

13 mai 2020

La US Cybersecurity and Infrastructure Security Agency (CISA) exhorte les organisations à corriger une multitude de vulnérabilités logicielles anciennes et nouvelles qui sont régulièrement exploitées par des cyber-acteurs et des cyber-criminels étrangers.

« Les cyber-acteurs étrangers continuent d'exploiter les vulnérabilités des logiciels connues du public, et souvent obsoletes, contre de vastes ensembles de cibles, notamment des organisations des secteurs public et privé. L'exploitation de ces vulnérabilités nécessite souvent moins de ressources par rapport aux exploits zero-day pour lesquels aucun correctif n'est disponible », a noté l'agence.

La liste des dix failles les plus exploitées entre 2016 et 2019 comprend sept affectant Microsoft (Office, Windows, SharePoint, .NET Framework), une affectant Apache Struts, une relative à Adobe Flash Player et une autre qui concerne Drupal.

Les vulnérabilités sont : CVE-2017-11882 ; CVE-2017-0199 ; CVE-2017-5638 ; CVE-2012-0158 ; CVE-2019-0604 ; CVE-2017-0143 ; CVE-2018-4878 ; CVE-2017-8759 ; CVE-2015-1641 ; CVE-2018-7600

Les professionnels de la sécurité informatique sont invités à utiliser cette liste en complément d'une liste similaire récemment compilée par Recorded Future, qui se concentre sur les dix vulnérabilités les plus exploitées par les cybercriminels en 2019 .

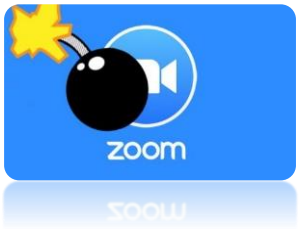
En plus de toutes ces failles, la CISA en signale plusieurs autres qui ont été fortement exploités en 2020 :

- CVE-2019-11510 affectant les serveurs VPN Pulse Secure
- CVE-2019-19781 affectant les appliances VPN Citrix

***Source :*** *https://bit.ly/2M4ws2R*

## Logiciels malveillants dans des faux installateurs de zoom

27 mai 2020




Deux exemples de logiciels malveillants ont été découverts qui se présentent comme des installateurs Zoom mais qu'ils s'avèrent être des logiciels malveillants.

- Un logiciel malveillant ayant des capacités de porte dérobée qui permet aux pirates d'accéder à distance.
- L'autre implique l'installation du botnet Devil Shadow sur des appareils compromis.

Les chercheurs en sécurité ont appelé Zoom « un désastre pour la protection de la vie privée » et ont noté que l'application était fondamentalement corrompue en raison de la prétendue mauvaise gestion des données par la société mère.

Zoom a également été critiqué pour sa fonction de suivi de l'attention qui permet à un hôte de voir si un utilisateur clique loin d'une fenêtre Zoom pendant 30 secondes ou plus […].

Il est à noter que ce n'est pas la première fois que Zoom fait face à des critiques sur sa gestion de la confidentialité et de la sécurité des données utilisateurs.

***Source :*** *https://bit.ly/2Xcpor3*

## Huawei nie toute implication dans une proposition de patch non sécurisé du noyau Linux

14 mai 2020

Huawei a nié, lundi 11 mai, toute implication officielle dans un correctif non sécurisé soumis au projet de noyau Linux. Un correctif qui a introduit une vulnérabilité "trivialement exploitable". Huawei affirme que l'employé a soumis le code dans le cadre d'un projet personnel, pas au nom de l'entreprise.

Le patch non sécurisé a été soumis au projet officiel du noyau Linux via sa liste de diffusion. Nommé HKSP (Huawei Kernel Self Protection), le correctif aurait introduit une série d'options de renforcement de la sécurité dans le noyau Linux.

Dans un article de blog publié le même jour, l'équipe de Grsecurity a déclaré avoir découvert que le correctif HKSP introduisait une vulnérabilité " trivialement exploitable " dans le code du noyau - si le correctif devait être approuvé.

Une mise à jour a également été ajoutée au projet HKSP à travers laquelle l'employé de Huawei a ajouté une clause de non-responsabilité […].

Le fait qu'un employé de Huawei ait écrit du code contenant des failles de sécurité n'est pas nouveau. Un rapport du gouvernement britannique l'année dernière a révélé que l' équipement de réseau Huawei était criblé de failles de sécurité qui passaient souvent des années sans recevoir de correctifs […].

La réaction de la communauté technologique dans ce cas particulier montre également le sentiment anti-Huawei, qui a été stimulé ces dernières années par d'innombrables problèmes de sécurité dans les produits de l'entreprise, des accusations de vol de propriété intellectuelle, des accusations de dissimulation de portes dérobées secrètes dans son firmware. et la crainte de l'Occident de voir le gouvernement chinois espionner les communications mondiales via l'équipement Huawei toujours populaire.

***Source :*** *https://zd.net/2BcWA9v*

# Evènements

## Evènements du mois

**AirGap 2020, en ligne**

**02 Mai 2020**

***https://bit.ly/2Aoxt2Q***

Une conférence virtuelle gratuite offerte par ThugCrowd, AirGap 2020 a été diffusée en direct sur Twitch. La conférence a particulièrement abordé « les bugs insolites et les approches non conventionnelles de la sécurité offensive ». Des présentations, des discussions entre des experts en sécurité et les participants, ainsi qu'un hackathon (Ch0pp3d) étaient au programme.

La conférence a été enregistrée et publiée sur la chaine YouTube (Thug Crowd).

**LevelUp 0x06, en ligne**

**09 Mai 2020**

***https://bit.ly/2ZOC8pC***

La conférence en direct sur la sécurité des informations de Bugcrowd s'est déroulée en ligne via YouTube, Twitch et Discord. Les conférenciers ont présenté des informations de pointe sur la cybersécurité, la recherche sur la sécurité et les primes de bugs. Les sessions couvraient des sujets allant des conseils et astuces de carrière et professionnels aux astuces de piratage automobile, aux comptes personnels de piratage offensif et aux derniers outils et technologies en matière de ceybersécurité.

**Blacks in Cybersecurity Virtual Conference 2020**

**16 Mai 2020**

***https://bit.ly/2XGDFLU***

Blacks in Cybersecurity ™ est un groupe de rencontres et de conférences axés sur la mise en évidence et l'élévation des minorités ethniques en matière de cybersécurité. La conférence virtuelle Blacks in Cybersecurity 2020 a proposé une gamme impressionnante de conférenciers et de panels couvrant des sujets tels que la carrière en cybersécurité, l'analyse des logiciels malveillants pour les intervenants en cas d'incident, la biocybersécurité, la stratégie de sécurité du cloud, etc. Les conférences sont enregistrées et ont été publiées sur la chaîne YouTube (Blacks In Cybersecurity Conference) du groupe pour une visualisation à la demande.

| | |
|---|---|
| **Reference** | ANPT-2020-BV-05 |
| **Titre** | Bulletin de veille N°5 |
| **Date de version** | 31 Mai 2020 |
| **Contact** | ssi@anpt.dz |