BULLETIN DE VEILLE N°8

ANPT-2020-BV-08

«Pour réussir la transformation numérique, transformez la gestion globale des risques et la cybersécurité en facteurs de différenciation commerciaux clés.» -Stéphane Nappo-

Août 2020

Alertes de sécurité

Microsoft

Faille d'usurpation de Windows activement exploitée corrigée deux ans après la divulgation

17 août 2020

La vulnérabilité d'usurpation de Windows activement exploitée a été corrigée la semaine dernière par Microsoft. Elle était connue depuis plus de deux ans, selon des chercheurs en cyber sécurité.

Les mises à jour du mardi correctif d'août 2020 de Microsoft ont corrigé 120 vulnérabilités, y compris un zero-day d'Internet Explorer qui a suivi une faille Windows dans les attaques liées au hacker DarkHotel, et un problème d'usurpation de Windows.

Un attaquant peut exploiter la vulnérabilité pour contourner les fonctionnalités de sécurité et charger des fichiers mal signés, indique Microsoft dans son avis. Les chercheurs ont analysé le CVE-2020-1464 après que Microsoft a publié son correctif et ont remarqué qu'il s'agissait d'une vulnérabilité connue depuis des années et que Microsoft a refusé de la corriger jusqu'à maintenant.

Il est recommandé d'appliquer les mises à jour publier par Microsoft.

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

Amazon

Amazon Alexa Bugs a permis aux pirates d'installer des compétences malveillantes à distance

13 août 2020

Les chercheurs en cybersécurité de Check Point ont révélé de graves vulnérabilités de sécurité dans l'assistant virtuel Alexa d'Amazon qui pourraient le rendre vulnérable à un certain nombre d'attaques malveillantes.

Selon un nouveau rapport , les «exploits auraient pu permettre à un attaquant de supprimer ou d'installer des compétences sur le compte Alexa de la victime ciblée, d'accéder à son historique vocal et d'acquérir des informations personnelles via une interaction de compétences lorsque l'utilisateur appelle la compétence installée. »

Check Point a déclaré que les failles provenaient d'une politique CORS mal configurée dans l'application mobile Alexa d'Amazon, permettant ainsi aux potentiels attaquants d'effectuer des injections de code sur un sous-domaine Amazon et de réaliser une attaque inter domaine sur un autre sous-domaine Amazon.

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

Cisco

Vulnérabilité des informations d'identification par défaut sur des produit Cisco

20 août 2020

Les tests de sécurité interne menés par Cisco ont révélé que les images groupées WAAS virtuel (vWAAS) avec Enterprise NFV Infrastructure Software (NFVIS) pour les appliances ENCS 5400-W et 5000-W incluent un mot de passe statique par défaut.

La vulnérabilité référencée CVE-2020-3446 peut être exploitée par un attaquant distant et non authentifié en utilisant ce compte par défaut pour se connecter à l'interface de ligne de commande NFVIS avec des privilèges d'administrateur […].

Cisco a également corrigé un problème de grande gravité dans l'implémentation du protocole de découverte des caméras IP de la série Video Surveillance 8000 qui pourrait permettre à un attaquant adjacent non authentifié d'exécuter du code arbitraire et/ou DoS.

La société a également publié des avis concernant de nombreuses vulnérabilités de gravité moyenne affectant Webex, Data Center Network Manager, les commutateurs Small Business, Vision Dynamic Signage Director et plusieurs autres produits. Cisco affirme ne pas avoir connaissance d'attaques exploitant ces vulnérabilités à ce jour.

Source : *https://bit.ly/2YPuv14*

Google

Risque de malware par le biais de fichiers partagés sur Google Drive,

25 août 2020

Google Drive est victime d'une faille qui peut être exploitée pour installer des malwares sur votre ordinateur. Cette vulnérabilité est liée à une négligence dans la gestion des versions de fichiers sur le service de stockage.

Un chercheur en cybersécurité a montré comment la fonctionnalité de gestion des versions de fichiers peut être exploitée par des personnes malintentionnées pour propager des programmes malveillants. En effet, la fonctionnalité de gestion des versions des fichiers partagés et notamment de remplacer une ancienne version d'un fichier par un nouveau sans modifier le lien de partage, a introduit cette vulnérabilité. Google Drive ne vérifie pas les extensions de fichier lorsque vous téléchargez une nouvelle version du document déjà existant. Le fichier d'origine peut ainsi être remplacé par un exécutable le plus simplement du monde. Pire, Google Drive conserve l'aperçu du fichier d'origine et n'indique pas les modifications qui y ont été nouvellement apportées.

Le chercheur A Nikoci affirme avoir informé Google de sa découverte, mais la faille n'a toujours pas été corrigée. Nous vous recommandons donc de ne télécharger que des documents partagés venant de personnes de confiance. Les fichiers publics doivent absolument être évités

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

Google corrige un bug de Gmail permettant aux attaquants d'envoyer des e-mails falsifiés

20 août 2020

Google a corrigé un bug critique affectant Gmail et G Suite qui aurait permis aux attaquants d'envoyer des e-mails malveillants usurpés comme n'importe quel autre utilisateur de Google ou client d'entreprise.

Selon Allison Husain, chercheuse en cyber sécurité qui a décelé et rapporté le problème à Google en avril dernier, le bug permet également aux hackers de rendre en apparence les emails frauduleux conformes à la Sender Policy Framework (SPF) et à la Domain-based Message Authentication, Reporting and Conformance (DMARC) – les deux étant des normes de sécurité de messagerie très avancées.

Google n'a pas réussi à résoudre le problème signalé par Husain pendant 137 jours.

Suite à cela, Husain a publié les détails du bug et un PoC sur son blog. Quelques heures après la publication, Google a déclaré avoir déployé des mesures d'atténuation afin de bloquer toute attaque tirant parti du problème signalé, en attendant le déploiement des correctifs finaux en septembre.

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

Intel

Vulnérabilité d'élévation de privilèges non corrigée dans Intel Driver & Support Assistant.

26 août 2020

Une vulnérabilité zero-day a été divulguée sans correctif par le conseiller en sécurité Anders Kusk.

La vulnérabilité référencée CVE-2020-12302 d'élévation de privilèges réside dans Intel Driver & Support Assistant.

Selon le chercheur, après avoir contacté Intel, il a été informé que la vulnérabilité serait corrigée dans 60 jours ou plus tôt. Au cours des 60 jours, plusieurs nouvelles versions de l'application ont été publiées, du 20.5.20 au 20.8.30.6.

Cependant, la vulnérabilité est toujours présente dans la dernière version. Versions affectées :

- 20.5.20 au moment de la découverte.
- 20.8.30.6 au moment de la divulgation publique.

Veuillez trouver dans la source plus de détails sur la vulnérabilité, ainsi le PoC.

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

Qualcomm

Les vulnérabilités du chipset Qualcomm mettent en danger des millions de téléphones Android

18 août 2020

Check Point, une société de cybersécurité a découvert que le DSP (Digital Signal Processor) utilisé dans le chipset Qualcomm Snapdragon a le code vulnérable qu'il appelle «Achilles». Celui-ci peut être utilisés comme un outil d'espionnage sur les téléphones.

Une application peut contourner les mesures de sécurité habituelles et peut ensuite accéder aux photos, vidéos, GPS et données de localisation du téléphone et cela sans que le propriétaire ne le sache. L'attaquant peut également verrouiller le téléphone avec toutes les données stockées, le rendant inutile. Il peut également être utilisé pour stocker des logiciels malveillants inconnus et inamovibles sur l'appareil […].

Dans un communiqué, Qualcomm a déclaré avoir travaillé dur pour valider et résoudre les problèmes. Il a également ajouté que la société n'a trouvé aucune preuve de l'exploitation de la vulnérabilité d'Achille sur le ccber espace.

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

TeamViewer

Une faille TeamViewer risque une exposition des mots de passe

20 août 2020

Une vulnérabilité dans l'application TeamViewer pourrait permettre à des acteurs malveillants de voler des mots de passe.

La faille référence CVE-2020-13699 a été découverte dans la version de bureau de l'application pour Windows avant la 15.8.3. En exploitant cette faiblesse, les acteurs malveillants authentifiés opérant à distance pourraient exécuter du code sur les systèmes des victimes ou déchiffrer leurs mots de passe

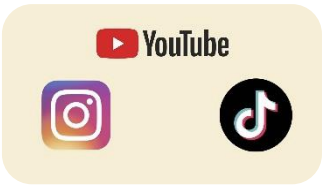
TeamViewer […]. Les victimes pourraient également être persuadées de se rendre sur un site Web spécifique mis en place par des pirates informatiques pour voler des informations d'identification ou des données personnelles. Il est recommandé aux entreprises de protéger leur système d'exploitation en se tenant au courant des dernières mises à jour de sécurité.

Source : *https://bit.ly/31w1hG2*

Actualité

Des centaines de millions de comptes Instagram, TikTok et YouTube compromis par une violation de données

21 août 2020



Des chercheurs en sécurité ont découvert une base de données exposée en ligne qui contient des données extraites des profils de médias sociaux de près de 235 millions d'utilisateurs Instagram, TikTok et YouTube (191 millions d'enregistrements ont été extraits d'Instagram, 42 millions de TikTok et près de 4 millions de YouTube).

Pour ceux qui ne connaissent pas cette pratique, le web scraping est une technique automatisée utilisée pour collecter des données à partir de sites Web. Elle est souvent employée par des sociétés d'analyse dans le but de créer de grandes bases de données d'informations sur les utilisateurs. Bien que cette pratique soit légale, elle est strictement interdite par les sociétés de médias sociaux car elle met en danger la vie privée de leurs utilisateurs et leurs données.

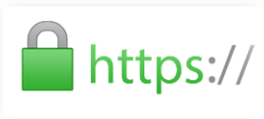
Le lead chercheur de Comparitech, Bob Diachenko, a découvert trois copies identiques de la base de données exposée en ligne au début du mois d'août. Après avoir examiné la base de données, Diachenko et son équipe ont appris qu'elle appartenait à une société appelée *Deep Social* qui a cessé ses activités.

Bien qu'il ne soit pas illégal de récupérer les données des utilisateurs sur les sites de médias sociaux, ne pas sécuriser ces données après leur collecte présente un risque sérieux pour les utilisateurs concernés, car les cybercriminels pourraient utiliser les informations collectées pour personnaliser leurs attaques selon les cibles.

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

HTTPS garantit-il un site web sûr ?

25 août 2020



L'application Web est passée du statut de référentiel d'informations contenant des documents statiques à des applications hautement fonctionnelles qui intègrent le flux bidirectionnel d'informations entre le serveur et le navigateur.

[…] De nombreuses personnes ont été amenées à croire que l'accès à une application Web HTTPS est une garantie que vous naviguez en toute sécurité, mais la vérité demeure, nous sommes tous exposés aux risques d'Internet malgré l'utilisation généralisée de HTTPS sur les applications Web […].

Selon OWASP (Open Web Application Security Project), les 10 principales vulnérabilités en 2020 sont

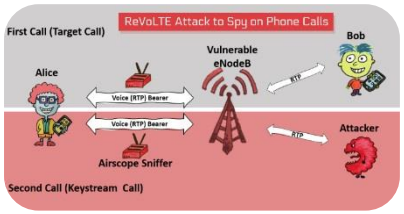
- Injection
- Authentification cassée
- Exposition des données sensibles
- Entités externes XML
- Contrôle d'accès cassé
- Erreurs de configuration de sécurité
- Scripts intersites (XSS)
- Désérialisation non sécurisée
- Utilisation de composants avec des vulnérabilités connues
- Journalisation et surveillance insuffisantes

Parmi la liste susmentionnée des 10 principales vulnérabilités Web, HTTPS empêche uniquement l'exposition aux données sensibles (certaines autres attaques peuvent toujours rendre l'application Web exposée de manière critique à ces vulnérabilités, par exemple l'injection SQL) en appliquant le cryptage sur les communications mais ne peut pas empêcher les 9 autres de la liste et bien d'autres non mentionnés ici. Pour cette raison, surfer sur Internet sur HTTPS ne garantit pas qu'un site Web soit sûr et sécurisé.

Source : *https://bit.ly/31uc4QV*

L'attaque ReVoLTE rompt le cryptage des appels VoLTE.

14 août 2020



Une équipe de chercheurs a récemment fait état d'un moyen de contourner le cryptage des appels enregistrés effectués à l'aide du protocole Voice over LTE (VoLTE).

Surnommée ReVoLTE, la technique exploite une faille dans l'implémentation que l'on trouve aujourd'hui du LTE par les opérateurs de réseaux cellulaires […].

Parlant de la faille, supposons donc que je passe un appel que les attaquants veulent espionner. Dans ce scénario, dès que je mets fin à mon appel, l'attaquant pourrait passer un deuxième appel à partir de sa fin en quelques secondes, ce qui utiliserait le même flux de clé utilisé lors de mon premier appel et lui donnerait ainsi la possibilité de connaître le flux de clé. En utilisant ces informations nouvellement obtenues, ils pouvaient maintenant déchiffrer mon premier appel enregistré. Cependant, tout cela nécessite plus qu'un simple ordinateur. Comme l'expliquent les chercheurs dans leur rapport [PDF],

Actuellement, les prestataires de services ont été informés de la vulnérabilité par le biais du programme de divulgation coordonnée de la vulnérabilité (CVD) de la GSMA et la faille aurait dû être corrigée. Néanmoins, nous avons de bonnes raisons de croire que les entreprises de téléphonie mobile dans les régions du monde où la confidentialité n'a pas beaucoup d'importance n'auraient pas été prompts à déployer des correctifs et il est donc nécessaire que les communautés de sécurité de ces pays poussent ces entreprises à le faire.

Source : *https://bit.ly/32mG7cI*

Certains clients de messagerie sont vulnérables aux attaques via des liens 'mailto'

18 août 2020

Une technologie moins connue sous le nom de liens « mailto » peut être utilisée de manière abusive pour lancer des attaques contre les utilisateurs de clients de bureau de messagerie […].

Mailto fait référence à des types de liens spéciaux, généralement pris en charge par les navigateurs Web ou les clients de messagerie. Ce sont des liens qui, lorsqu'ils sont cliqués, ouvrent une nouvelle fenêtre de rédaction / réponse d'e-mail plutôt qu'une nouvelle page Web […].

Mais dans un article de recherche intitulé « Mailto : Me Your Secrets [PDF] », des universitaires ont déclaré que quelque paramètres permettent des attaques contre leur utilisateurs […].

Les universitaires affirment que les attaquants peuvent envoyer des e-mails contenant des liens mailto piégés ou placer des liens mailto piégés sur des sites Web qui, lorsqu'ils sont cliqués, pourraient ajouter subrepticement des fichiers sensibles à la fenêtre de courrier électronique […].

L'équipe de recherche a déclaré avoir testé 20 clients de messagerie pour leur scénario d'attaque et constaté que quatre clients étaient vulnérables. Cette liste comprenait :

- Evolution, le client de messagerie par défaut pour l'environnement de bureau GNOME sous Linux (voir CVE-2020-11879)
- KMail, le client de messagerie par défaut pour les environnements de bureau KDE sous Linux (voir CVE-2020-11880)
- Notes IBM / HCL sous Windows (voir CVE-2020-4089)
- Anciennes versions de Thunderbird sous Linux (maintenant patché)

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

Transparent Tribe APT cible le gouvernement et l'armée en infectant des périphériques USB

20 août 2020

Transparent Tribe est impliqué dans des campagnes contre le personnel gouvernemental et militaire, révélant un nouvel outil conçu pour infecter les périphériques USB et se propager à d'autres systèmes.

Transparent Tribe se concentre sur la surveillance et l'espionnage et pour atteindre ces objectifs, le groupe fait constamment évoluer sa boîte à outils en fonction de la cible visée, a déclaré Kaspersky dans un article de blog jeudi.

La chaîne d'attaque commence de manière typique, via des e-mails de spear-phishing. Les messages frauduleux sont envoyés avec des documents Microsoft Office malveillants contenant une macro intégrée qui déploie la charge utile principale du groupe, le Crimson Remote Access Trojan (RAT) […].

Transparent Tribe utilise également d'autres logiciels malveillants .NET et un cheval de Troie en Python appelé Peppy, mais un nouvel outil d'attaque USB est particulièrement intéressant.

USBWorm est composé de deux composants principaux, un voleur de fichiers pour les lecteurs amovibles et une fonction de ver pour accéder à de nouvelles machines vulnérables.

Si une clé USB est connectée à un PC infecté, une copie du cheval de Troie est silencieusement installée sur le lecteur amovible. Le logiciel malveillant répertorie tous les répertoires sur un lecteur, puis une copie du cheval de Troie est enterrée dans le répertoire du lecteur racine. L'attribut du répertoire est alors changé en "caché" et une fausse icône Windows est utilisée pour inciter les victimes à cliquer et à exécuter la charge utile lorsqu'elles tentent d'accéder aux répertoires.

Plus de 200 échantillons de composants Transparent Tribe Crimson ont été détectés entre juin 2019 et juin 2020 […].

Source : *https://zd.net/31sAiuW*

Le botnet Lucifer peut désormais cibler les périphériques Linux

21 août 2020

Les chercheurs de l' Unité 42 de Palo Alto Network ont d' abord remarqué le botnet Lucifer en juin, notant que le malware profite de nombreuses vulnérabilités non corrigées dans les appareils Windows, ce qui permet ensuite aux attaquants d'exécuter du code arbitraire […].

Désormais, les opérateurs derrière le botnet Lucifer ont créé une version qui peut cibler les systèmes Linux, ce qui peut renforcer la capacité des attaquants à lancer des attaques DDoS, y compris des attaques par inondation basées sur ICMP, TCP et UDP, selon Netscout […].

Les chercheurs de Netscout ont également constaté que la version mise à jour de Lucifer conçue pour Windows a ajouté des fonctionnalités. Il installe désormais également Mimikatz, un script PowerShell utilisé pour voler les informations d'identification et augmenter les privilèges sur les appareils Windows compromis.

Lorsque l'Unité 42 a découvert Lucifer pour la première fois, les chercheurs ont découvert que le botnet utilisait des méthodes de force brute visant les ports vulnérables pour deviner des

combinaisons de noms d'utilisateur et de mots de passe pour lancer l'attaque initiale. Le logiciel malveillant tirera également parti d'exploits bien connus, tels que EternalBlue, pour lui permettre d'exécuter du code arbitraire dans l'appareil compromis.

D'autres botnets, tels que Kaiji, semblent également être conçus pour cibler les systèmes Linux.

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

Evènements

Evènements du mois

Cloud Security Summit

Virtuel, 13 août 2020

https://bit.ly/2YEkG61

L'évènement a permis aux participants d'interagir avec les principaux fournisseurs de solutions et d'autres utilisateurs finaux chargés de sécuriser divers environnements et services cloud. Le but de cet évènement est d'aider les organisations à apprendre à utiliser les outils, les contrôles et les modèles de conception nécessaires pour sécuriser correctement les environnements cloud.

Les sessions qui ont été présenté lors de l'évènement sont :

- Augmentation des services de sécurité cloud natifs pour atteindre une sécurité de niveau entreprise
- Mesure et atténuation du risque de mouvement latéral
- Weathering the Storm : Cyber AI pour Cloud et SaaS
- La sécurisation du cloud nécessite une politique de réseau et une segmentation
- Gérer la confiance numérique à l'ère des mégabreaches du cloud
- La montée en puissance de Secure Access Service Edge (SASE)
- Conversation au coin du feu avec Gunter Ollmann , CSO de la division Cloud and AI Security de Microsoft

Evènements à venir

CISO Africa, Live, 22-23 Septembre 2020,

Virtuel, Gauteng, South Africa

https://bit.ly/3lph9SA

Cet événement Cyber africain sera virtuel et diffusé depuis Gauteng, Afrique du Sud. Pour ceux qui travaillent dans le domaine de la cybersécurité en Afrique. Vous pouvez considérer CISO Africa comme un événement de premier plan de niveau CXO pour les professionnels d'InfoSec de haut niveau.

Cette conférence 100% virtuelle qui mettra en relation les leaders africains de la sécurité avec les fournisseurs de solutions les plus avant-gardistes au monde, dans un contexte de contenu de pointe. À la maison, au bureau ou sur la route. Il s'agit d'un événement hautement recommandé aux professionnels et aux passionnés de la cybersécurité.

Reference	ANPT-2020-BV-08
Titre	Bulletin de veille N°8
Date de version	31 Août 2020
Contact	ssi@anpt.dz