BULLETIN DE VEILLE N°10

ANPT-2020-BV-10

« Oublier la cyber sécurité, c'est rouler à 200 km/h à moto sans casque »
-Guillaume Poupard-

Octobre 2020

Alertes de sécurité

Google

Google Patches Bug Zero-Day exploité activement dans le navigateur Chrome

21 octobre 2020

Google a publié une mise à jour de son navigateur Chrome qui corrige une vulnérabilité zero-day dans la bibliothèque de rendu de polices FreeType qui était activement exploitée dans la nature.

Le chercheur en sécurité Sergei Glazunov de Google Project Zero a découvert le bug qui est classé comme un type de faille de corruption de mémoire appelé débordement de tampon de tas dans FreeType.

Google avait déjà publié une mise à jour de canal stable, Chrome version 86.0.4240.111, qui déploie cinq correctifs de sécurité pour Windows, Mac et Linux - parmi lesquels un correctif pour le bug zero-day suivi sous la référence CVE-2020-15999 et considéré comme un risque élevé.

Les utilisateurs doivent s'assurer de mettre à jour leur navigateur chrome.

Source : *https://bit.ly/31Fwzd4*

Microsoft

Patch Microsoft : Méfiez-vous du Bad Neighbor

16 octobre 2020

Les spécialistes de la cybersécurité ont divulgué plusieurs détails sur une faille de sécurité récemment découverte appelée «Vulnérabilité Bad Neighbor ». La communauté d'experts recommande aux utilisateurs d'installer les correctifs disponibles pour empêcher une attaque.

Selon l'US Cyber Command, les utilisateurs de produits Microsoft devraient installer la mise à jour pour corriger cette faille dès que possible. Le patch a été publié dans le cadre du Patch Tuesday de Microsoft cette semaine.

La vulnérabilité CVE-2020-16898 d'exécution de code à distance qui réside dans Windows TCP / IP peut également générer une condition de déni de service (DoS). Un pirate informatique distant non authentifié ne peut l'exploiter qu'en envoyant des paquets d'annonce de routeur ICMPv6 malveillants à une machine Windows vulnérable.

Le rapport mentionne que Bad Neighbor affecte les versions du système d'exploitation client (Windows 10 1709 à 2004) et serveur (Windows Server 1903 à 2004 et Windows Server 2019), ce qui en fait une vulnérabilité critique pour toutes les implémentations Windows modernes. La société a déjà fourni aux membres du programme Microsoft Active Protections Program (MAPP) une preuve de concept de l'exploit, en outre, Sophos a également créé son propre exploit PoC.

Si vous ne parvenez pas temporairement à installer le correctif, Microsoft recommande de désactiver l'option Serveur DNS récursif ICMPv6 (RDNSS) sur Windows 10 1709 et versions ultérieures.

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

WordPress

WordPress déploie une mise à jour de sécurité forcée pour un bug dangereux dans un plugin populaire

21 octobre 2020

Une mise à jour forcée pour les sites WordPress exécutant le plugin Loginizer vers la version 1.6.4 de Loginizer.

Cette version contenait un correctif de sécurité pour un bug d'injection SQL dangereux qui aurait pu permettre à des pirates de prendre le contrôle de sites WordPress exécutant des versions plus anciennes du plugin Loginizer […].

Selon une description fournie par la base de données de vulnérabilité WPScan WordPress, le bug de sécurité réside dans le mécanisme de protection par force brute de Loginizer, activé par défaut pour tous les sites sur lesquels Loginizer est installé.

Pour exploiter ce bug, un attaquant peut essayer de se connecter à un site WordPress en utilisant un nom d'utilisateur WordPress mal formé dans lequel il peut inclure des instructions SQL […].

Etant donné que le plugin ne nettoie pas le nom d'utilisateur et laisse les instructions SQL intactes, cela permet aux attaquants distants d'exécuter du code contre la base de données WordPress – communément connue sous le nom d'attaque par injection SQL non authentifiée.

Le chercheur de sécurité qui a découvert le bug a également publié un simple script de preuve de concept (PoC).

Source : *https://zd.net/3or32h6*

Apple

Une vulnérabilité récemment découverte dans la puce de sécurité T2 d'Apple pourrait donner un accès root

05 octobre 2020

Une vulnérabilité récemment découverte affecte les systèmes macOS avec Intel processeur et puce T2. Le chercheur qui a découvert la vulnérabilité dit qu'elle n'est pas patchable et peut potentiellement donner un accès root aux attaquants […].

La bonne nouvelle est que les attaquants auront besoin d'un accès physique au système et devront utiliser des périphériques comme un câble USB-C malveillant ou tout autre insert matériel. De plus, la vulnérabilité peut concerner le contournement manuel des verrous de sécurité et du verrou d'activation intégré. L'accès à T2 accordera à l'attaquant l'accès à tous les privilèges d'exécution du noyau. Le chiffrement du disque peut empêcher l'attaque dans une certaine mesure. Cependant, les attaquants peuvent accéder aux claviers en injectant des keyloggers dans le firmware T2 […].

Les utilisateurs de Mac sont invités à utiliser Apple Configurator pour réinstaller bridgeOS sur la puce T2 et, surtout, ne pas laisser leur appareil sans surveillance. Ne branchez jamais un périphérique USB inconnu.

Source : *https://bit.ly/35wGN0z*

Linux

Les systèmes Linux risquent d'être préoccupés par la vulnérabilité Bluetooth de BleedingTooth

20 octobre 2020

Un chercheur en sécurité de Google a émis un avertissement concernant une série de vulnérabilités «zéro clic» dans la pile Bluetooth Linux.

Surnommée BleedingTooth, la collection de failles de sécurité pourrait permettre des attaques d'exécution de code à distance. Le problème affecte le noyau Linux 4.8 et supérieur, et peut être trouvé dans la pile de protocoles open-source BlueZ.

Sur GitHub, les chercheurs de Google partagent des détails sur BleedingTooth, le décrivant comme une "confusion de type basée sur le tas dans L2CAP".

Le chercheur en sécurité affirme que la vulnérabilité référencée CVE-2020-12351 est de haute gravité et propose un exemple de code comme preuve de concept qui fonctionne sur Ubuntu 20.04 LTS.

Sur Twitter, l'ingénieur en sécurité Andy Nguyen a partagé des nouvelles de la vulnérabilité, y compris une vidéo montrant la vulnérabilité zéro-clic en action.

Intel a publié son propre avis de sécurité sur la vulnérabilité et suggère aux utilisateurs d'installer une série de correctifs du noyau pour se protéger eux-mêmes et protéger leurs systèmes.

Source : *https://bit.ly/37IuvoQ*

Oracle

Un ensemble de 402 correctifs proposé par Oracle

21 octobre 2020

Oracle a publié son dernier lot trimestriel de correctifs pour l'année pour les failles de sécurité de ses produits.

Un bon nombre de vulnérabilités sont exploitables sans nécessiter de privilèges spéciaux, tels que ceux de la base de données Oracle TimesTen In-Memory (CVE-2018-11058, CVE-2017-5645, CVE-2019-1010239 et CVE-2019-0201). De même, 41 des vulns corrigés dans Oracle Communications «peuvent être exploitables à distance sans authentification, c'est-à-dire peuvent être exploités sur un réseau sans avoir besoin d'informations d'identification de l'utilisateur», pour reprendre les propres mots de Big Red.

La liste complète des mises à jour, qui font partie de l'exécution trimestrielle des correctifs critiques d'Oracle, peut être consultée sur son site Web. Des informations plus détaillées sont disponibles pour ceux qui disposent d'une connexion Oracle pour accéder à des notes de patch entièrement détaillées.

Le géant de la base de données recommande fortement aux clients de rester sur les versions activement prises en charge et d'appliquer les correctifs de sécurité Critical Patch Update le plus rapidement possible.

Source : *https://bit.ly/2Tqa1su*

Nvidia

Nvidia avertit les gameurs des graves failles de GeForce Experience

23 octobre 2020

Nvidia, qui fabrique des unités de traitement graphique (GPU) conviviales pour les jeux, a publié des correctifs pour deux failles de haute gravité dans la version Windows de son logiciel GeForce Experience.

La faille la plus grave des deux (CVE-2020-5977) peut conduire à une série d'attaques malveillantes sur les systèmes affectés- y compris l'exécution de code, le déni de service, l'élévation des privilèges et la divulgation d'informations.

Les versions de Nvidia GeForce Experience pour Windows antérieures à 3.20.5.70 sont affectées ; les utilisateurs sont invités à mettre à jour vers la version 3.20.5.70.

Les utilisateurs peuvent télécharger les mises à jour à partir de la page de téléchargement de GeForce Experience ou ouvrir le client pour appliquer automatiquement la mise à jour de sécurité.

Source : *https://bit.ly/3ciKLx0*

Actualité

Les pirates utilisent une fausse version de Netflix en arabe pour les attaques de phishing

26 octobre 2020

Des chercheurs de Kaspersky Cyber Security Solutions ont récemment découvert un groupe d'attaques de phishing qui exploitent un site Web malveillant déguisé en page Netflix en arabe […].

En utilisant le faux site Web, les pirates visent à récupérer les données de connexion des comptes Netflix par le biais d'attaques de phishing […].

D'autres risques surviennent lorsque les données de connexion sont les mêmes pour d'autres comptes importants, ce qui peut permettre à des criminels de pirater des comptes de réseaux sociaux ou des e-mails, et peut-être même des comptes bancaires.

Selon le centre d'aide de Netflix, il existe quelques moyens simples de protéger votre compte et vos informations personnelles :

✓ Utilisez un mot de passe propre à Netflix et modifiez-le régulièrement.
✓ N'utilisez pas le même mot de passe sur Netflix que celui que vous utilisez pour d'autres sites Web ou applications.
✓ La taille du mot de passe doit être d'au moins 8 caractères.
✓ Une combinaison de lettres, de chiffres et de symboles utilisant à la fois des lettres majuscules et minuscules.
✓ Difficile à deviner – évitez «mot de passe», «12345» ou vos informations personnelles (nom, anniversaire, adresse).

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

Waze de Google peut permettre aux pirates d'identifier et de suivre les utilisateurs

20 octobre 2020

Un chercheur en sécurité a découvert une faille API dans le logiciel de navigation qui lui permettait de suivre en temps réel les mouvements spécifiques des conducteurs à proximité et même d'identifier exactement qui ils étaient, a-t-il révélé dans un article de blog sur son site de recherche, «malgregator»,[...]

Gasper a déclaré que ses recherches avaient commencé assez innocemment lorsqu'il s'est rendu compte qu'il pouvait visiter Waze à partir de n'importe quel navigateur Web à l'adresse waze.com/livemap et a décidé de voir comment l'application implémentait les icônes des autres conducteurs à proximité. Il a découvert que non seulement Waze lui envoie les coordonnées des autres conducteurs à proximité, mais aussi que « les numéros d'identification (ID) associés aux icônes ne changeaient pas au fil du temps » […].

Des rumeurs selon lesquelles Waze et d'autres applications utilisant des informations provenant de la foule ne sont pas sécurisées ont déjà fait surface il y a plusieurs années avec un rapport (PDF) de chercheurs de l'Université de Santa Barbara. Ils ont découvert qu'une fois un utilisateur Waze était identifié, ils pouvaient faire écho à la position GPS de cette personne en créant un «cavalier fantôme». Cela donnerait à quelqu'un la possibilité de suivre virtuellement la victime via une attaque de l'homme du milieu, en rapportant ses positions GPS.

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

Sept navigateurs mobiles vulnérables aux attaques d'usurpation de la barre d'adresse

20 octobre 2020

Une vulnérabilité «d'usurpation de la barre d'adresse» fait référence à un bug dans un navigateur Web qui permet à un site Web malveillant de modifier sa véritable URL et d'en afficher une fausse à la place - généralement une pour un site légitime.

Les vulnérabilités d'usurpation de la barre d'adresse existent depuis les débuts du Web, mais elles n'ont jamais été aussi dangereuses qu'elles le sont aujourd'hui.

Dans un rapport publié par la société de cybersécurité Rapid7, dix nouvelles vulnérabilités d'usurpation de la barre d'adresse dans sept applications de navigateur mobile ont été divulguées.

Les navigateurs concernés incluent de grands noms comme Apple Safari, Opera Touch et Opera Mini, mais également des applications de niche telles que Bolt, RITS, UC Browser et Yandex Browser […].

Rapid7 estime que les attaques sont faciles à monter et recommande aux utilisateurs de mettre à jour leurs navigateurs dès que possible ou de passer à des navigateurs qui ne sont pas affectés par ces bugs.

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

GravityRAT espionne les SMS, photos et appels de ses victimes

22 octobre 2020

Les chercheurs de Kaspersky ont découvert que GravityRAT, initialement réservé aux ordinateurs sous Windows, s'attaque désormais aux appareils Android et aux Macs.

Développés par des pirates informatiques pakistanais depuis 2015, le trojan a été modifié pour étendre son champ d'action au cours des deux dernières années […].

Après enquête, Kaspersky a identifié plus de 10 versions différentes du malware dans la nature. Le logiciel malveillant se propage "sous couvert d'applications légitimes, telles que des applications de partage de fichiers sécurisées qui aideraient à protéger les appareils des utilisateurs contre les Trojans, ou via des lecteurs multimédia". Les chercheurs ne précisent pas si GravityRAT est parvenu à s'infiltrer sur le Play Store, la boutique d'applications de Google […].

Une fois que le malware est parvenu à entrer dans le téléphone ou l'ordinateur de ses victimes, il va méticuleusement collecter les données personnelles des utilisateurs, comme les SMS, l'historique des appels, les informations système du terminal ou la liste des adresses mails contactées. Ces informations peuvent être monnayées à prix d'or sur des marchés noirs du dark web […]. Il est recommandé de se protéger grâce à un antivirus Android.

***Source** : https://bit.ly/34vG3d4*

Ransomware Ryuk : la piste d'une attaque éclair contre Sopra Steria

23 octobre 2020

Le géant français des services informatiques Sopra Steria a subi une cyberattaque le 20 octobre 2020, qui aurait chiffré des parties de son réseau avec le logiciel de rançon Ryuk. Sopra Steria a confirmé dans un communiqué de presse officiel que la société a détecté une cyberattaque sur son réseau informatique, mais n'a pas fourni plus de détails. Mais les médias français ont indiqué que l'infrastructure Active Directory de Sopra Steria avait été compromise par les pirates informatiques à l'origine de l'attaque […].

Des sources qui connaissent des informations sur l'attaque ont déclaré à des médias que le réseau informatique de Sopra Steria était crypté par Ryuk ransomware, le même groupe qui a infecté en septembre l'Universal Health Services (UHS), un hôpital et un fournisseur de services de santé figurant au classement Fortune 500, et qui gère plus de 400 établissements de soins de santé aux États-Unis et au Royaume-Uni […].

Au cours des trois derniers mois, les attaques de logiciels rançonneurs ont augmenté de 50 % en moyenne dans le monde par rapport au premier semestre de 2020, d'après un rapport publié ce mois par les chercheurs de Check Point. Les chiffres semblent encore plus sombres pour certains pays, avec des attaques en hausse de 98 % aux États-Unis, 80 % au Royaume-Uni, 145 % en Allemagne, 36 % en France et 160 % en Espagne. Cette hausse aurait un lien avec l'apparition du covid-19.

***Source** : https://bit.ly/3ky488o*

FBI, CISA : Des pirates russes ont violé les réseaux du gouvernement américain, exfiltré des données

21 octobre 2020

Le gouvernement américain a déclaré qu'un groupe de pirates informatiques parrainé par l'État russe avait ciblé et violé avec succès les réseaux du gouvernement américain.

Des responsables gouvernementaux ont divulgué les hacks dans un avis de sécurité conjoint publié par la Cybersecurity and Infrastructure Security Agency (CISA) et le Federal Bureau of Investigation (FBI).

Les deux agences ont déclaré qu'Energetic Bear "avait réussi à compromettre l'infrastructure du réseau et, à compter du 1er octobre 2020, à exfiltrer les données d'au moins deux serveurs victimes" […].

Selon l'avis technique, des pirates informatiques russes ont utilisé des vulnérabilités connues du public pour violer les équipements de réseau, pivoter vers les réseaux internes, élever les privilèges et voler des données sensibles.

Les appareils ciblés comprenaient les passerelles d'accès Citrix (CVE-2019-19781), les serveurs de messagerie Microsoft Exchange (CVE-2020-0688), les agents de messagerie Exim (CVE 2019-10149), la vulnérabilité Zerologon dans les serveurs Windows (CVE-2020-1472) et les VPN SSL Fortinet (CVE-2018-13379) […].

Energetic Bear est également le même groupe de hackers qui a ciblé l'aéroport de San Francisco plus tôt ce printemps.

***Source** : https://zd.net/37N9oBP*

Géorgie : les données électorales touchées lors d'une attaque de ransomware

23 octobre 2020

Les gangs de ransomwares sont officiellement entrés dans la mêlée électorale de 2020, avec des informations faisant état de l'une des premières violations de la saison des votes, dans le comté de Hall, en Géorgie.

Bien que le comté ait déclaré que le processus de vote n'avait pas été affecté par l'attaque du ransomware, l'incident est un avertissement aux autres municipalités de verrouiller leurs systèmes, en particulier ces derniers jours précédant les élections […].

Pour protéger les systèmes à un moment aussi délicat, deux choses simples peuvent faire une grande différence : les correctifs et la formation des employés, selon Daniel Norman, analyste principal des solutions à l'Information Security Forum.

Les ransomwares sont en hausse dans le monde entier grâce à la pandémie, en hausse de plus de 109% par rapport à l'année dernière, selon le rapport sur les cybermenaces 2020 de SonicWall.

***Source** : https://bit.ly/3dUA4l4*

Evènements

Evènements du mois

EuroCACS 2020, Virtuel

28 - 30 Octobre 2020

https://bit.ly/3j9aevg

EuroCACS 2020 Virtual a rassemblé des acteurs du domaine de l'audit, de la sécurité, de la conformité, des risques, de la confidentialité, du contrôle et de l'informatique, issus d'un large éventail d'industries, notamment ; finance, banque, services technologiques, gouvernement, assurance, médical et plus encore.

Plus de 40 sessions ont fourni aux participants des informations sur les dernières tendances réglementaires, un aperçu des menaces de cybersécurité et les connaissances des autres professionnels qui assistent à la conférence.

Les sessions virtuelles EuroCACS 2020 ont été réparties en trois niveaux d'apprentissage, une formation technique et des compétences générales, des conférences, des tables rondes et plus encore.

Risques de sécurité sur les Technologies Opérationnels (OT) : accès et maintenance à distance, Webnair

29 Octobre 2020, Virtuel

https://bit.ly/2TpyrCx

Les cyberattaques contre les systèmes ICS et SCADA peuvent avoir des conséquences catastrophiques sur la sécurité, la disponibilité et la fiabilité des travailleurs, des opérations et des chaînes de valeur. Il est donc essentiel de protéger ces systèmes et réseaux contre les menaces, surtout maintenant, lorsque le travail à distance est devenu la norme à l'époque du Corona.

L'accès à distance est un sujet sensible et n'a pas toujours été organisé correctement. Dans ce webinaire co-organisé par Trinity Digital Security et Secura, des experts en sécurité OT ont abordé les pièges courants, les leçons tirées des études de cas précédentes et les recommandations pour créer des environnements OT sécurisés.

Evènements à venir

CyberTech Africa

22-24 Novembre 2020, Kigali, Rwanda

https://bit.ly/3jwPopb

La Cybertech Africa servira de lieu de rencontre pour les décideurs locaux et internationaux pour tout ce qui concerne la cybersécurité et l'innovation. L'événement offre une plate-forme pour découvrir, discuter et analyser les défis, les solutions et les développements technologiques qui sont à la pointe de l'innovation et de la cybersécurité mondiales. Les sujets incluront la fintech, la confidentialité, l'IoT, les infrastructures critiques, la cyber-sensibilisation et bien plus encore ! Combinant l'écosystème local et l'expertise internationale, les orateurs comprennent des hauts fonctionnaires et des dirigeants de l'industrie.

Reference	ANPT-2020-BV-10
Titre	Bulletin de veille N°10
Date de version	31 Octobre 2020
Contact	ssi@anpt.dz