BULLETIN DE VEILLE N°9

ANPT-2020-BV-09

« Avec un grand pouvoir viennent de grandes responsabilités. »
– BENJAMIN PARKER, SPIDER-MAN-

Septembre 2020

Alertes de sécurité

Microsoft

La commande *Finger* de Windows 10 peut être utilisée de manière abusive pour voler des fichiers

15 septembre 2020

Le dernier ajout est finger.exe, une commande fournie avec Windows pour récupérer des informations sur les utilisateurs sur des ordinateurs distants exécutant le service ou le démon Finger. La communication s'effectue via le protocole de communication réseau Name / Finger, sans que Windows Defender détecte l'activité anormale.

Le chercheur en sécurité John Page a découvert que la commande Microsoft Windows TCPIP Finger peut également fonctionner comme un téléchargeur de fichiers et un serveur de commande et de contrôle de fortune (C3) qui peut servir à envoyer des commandes et à exfiltrer des données […].

Selon un article de blog, le port 79, utilisé par le protocole Finger, est souvent bloqué au sein d'une organisation […]. Cependant, un attaquant disposant de privilèges suffisants peut contourner la restriction en utilisant Windows NetSh Portproxy, qui agit comme un redirecteur de port pour le protocole TCP.

Le chercheur a créé des scripts de preuve de concept (PoC) - *DarkFinger.py* pour le C2 et le côté client *DarkFinger-Agent.bat* - et les a publiés pour démontrer la double fonctionnalité de finger.exe.

Source : ***https://bit.ly/35Sz52C***

Microsoft Defender peut ironiquement être utilisé pour télécharger des logiciels malveillants

02 septembre 2020

Une mise à jour récente de la solution antivirus Microsoft Defender de Windows 10 lui permet ironiquement de télécharger des logiciels malveillants et d'autres fichiers sur un ordinateur Windows.

Les fichiers légitimes du système d'exploitation qui peuvent être exploités à des fins malveillantes sont connus sous le nom de fichiers binaires ou LOLBIN.

Découverte par le chercheur en sécurité Mohammad Askar , une mise à jour récente de l'outil de ligne de commande de Microsoft Defender **MpCmdRun.exe** inclut désormais un nouvel ***-DownloadFileargument*** de ligne de commande.

Cette directive permet à un utilisateur local d'utiliser l'utilitaire de ligne de commande Microsoft Antimalware Service (MpCmdRun.exe) pour télécharger un fichier à partir d'un emplacement distant.

Dans les tests menés par BleepingComputer.com, cette fonctionnalité a été ajoutée à Microsoft Defender dans la version 4.18.2007.9 ou 4.18.2009.9.

La bonne nouvelle est que Microsoft Defender détectera les fichiers malveillants téléchargés avec MpCmdRun.exe, mais on ne sait pas si d'autres logiciels AV permettront à ce programme de contourner leurs détections […].

Source: *https://bit.ly/32QLx1b*

Appliquer le Patch en urgence ! L'Exploit de Microsoft Netlogon

15 septembre 2020

Des chercheurs de la société néerlandaise de cybersécurité Secura ont publié un exploit de «preuve de concept» pour une vulnérabilité dans le protocole Netlogon que Microsoft utilise pour authentifier les utilisateurs dans un domaine […].

Cette vulnérabilité pourrait permettre à un attaquant d'usurper l'identité de n'importe quel ordinateur, y compris le contrôleur de domaine lui-même, et exécuter des appels de procédure à distance en son nom.

Rapid7 a conseillé les utilisateurs de « corriger la faille en urgence en raison de la gravité de la vulnérabilité, de la disponibilité d'un PoC facilement armable et de la facilité d'exploitation ».

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

Bluetooth

Des milliards d'appareils vulnérables à la nouvelle faille de sécurité Bluetooth « BLESA »

15 septembre 2020

Des milliards de smartphones, tablettes, ordinateurs portables et appareils IoT utilisent des piles de logiciels Bluetooth qui sont vulnérables à une nouvelle faille de sécurité.

Nommée BLESA (Bluetooth Low Energy Spoofing Atack), la vulnérabilité affecte les appareils exécutant le protocole Bluetooth Low Energy (BLE).

Deux failles de sécurité critiques dans le mécanisme d'authentification de la couche de liaison BLE exposent les périphériques Bluetooth à l'attaque BLESA. Ces vulnérabilités permettent à un attaquant de se faire passer pour un serveur BLE et de fournir des données usurpées à un autre appareil précédemment couplé.

Les chercheurs ont découvert que BlueZ (appareils IoT basés sur Linux), Fluoride (Android) et la pile iOS BLE étaient tous vulnérables aux attaques BLESA.

Apple a attribué le CVE-2020-9770 à la vulnérabilité et l'a corrigée. Certains équipements IoT aux ressources limitées qui ont été vendus au cours de la dernière décennie et ont déjà été déployés sur le terrain aujourd'hui ne sont pas livrés avec un mécanisme de mise à jour intégré, ce qui signifie que ces appareils resteront en permanence non corrigés.

Des détails supplémentaires sur l'attaque BLESA sont disponibles ici.

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

Firefox

Firefox bug permet de détourner les navigateurs mobiles à proximité via WiFi

18 septembre 2020

Mozilla a corrigé un bug dont on pouvait abuser pour détourner tous les navigateurs Firefox pour Android sur le même réseau WiFi et forcer les utilisateurs à accéder à des sites malveillants, tels que des pages de phishing.

Le bug a été découvert par Chris Moberly, un chercheur en sécurité australien travaillant pour GitLab. Le chercheur a aussi publié un code de preuve de concept (PoC).

Pour mieux comprendre comment ce bug pourrait être abusé, imaginons un scénario où un pirate se trouve dans un aéroport ou un centre commercial, se connecte au réseau WiFi, puis lance un script sur son ordinateur portable qui envoie un spam sur le réseau avec des paquets SSDP mal formés.

Tout propriétaire d'Android utilisant un navigateur Firefox pour naviguer sur le Web pendant ce type d'attaque verrait son navigateur mobile détourné et dirigé vers un site malveillant, ou forcé d'installer une extension Firefox malveillante.

Le bug a été corrigé dans Firefox 79. Un porte-parole de Mozilla a recommandé aux utilisateurs de passer à la dernière version de Firefox pour Android pour être en sécurité.

Source : *https://zd.net/33R8gEe*

Philips

Vulnérabilités du logiciel de surveillance des patients identifiées

14 septembre 2020

Les autorités fédérales américaines et le fabricant de dispositifs médicaux Philips ont émis des alertes de sécurité concernant des vulnérabilités de sécurité dans certains des logiciels de surveillance des patients de l'entreprise.

Une exploitation réussie de ces vulnérabilités pourrait entraîner un accès non autorisé, une interruption de la surveillance et de la collecte des informations d'accès et / ou des données des patients. Cependant, pour réussir à les exploiter, un attaquant devrait avoir un accès physique aux stations de surveillance et aux moniteurs de patients ou accéder au réseau des dispositifs médicaux.

Philips prévoit de publier une série de mises à jour pour corriger toutes les vulnérabilités signalées pour les produits concernés.

En attendant la disponibilité de ces correctifs, Philips recommande aux organisations de santé de suivre quelques mesures préventives (Voir la source).

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

Android

Android corrige des vulnérabilités système critiques

20 août 2020

Google a corrigé deux vulnérabilités critiques dans le composant système Android dans le cadre de la nouvelle série de correctifs de sécurité de septembre 2020.

Les failles System critiques susmentionnées référencées comme CVE-2020-0380 et CVE-2020-0396 peuvent conduire à l'exécution de code à distance et à la divulgation d'informations, respectivement.

Les systèmes affectés sont Android 8.0, 8.1, 9 et 10.

Le patch comprends, notamment, d'autres corrections, consultez le bulletin pour plus de détails.

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

Apple

Un bug Apple permet l'exécution de code sur iPhone, iPad et iPod

17 septembre 2020

La sortie d'iOS 14 et d'iPadOS 14 apporte des correctifs de 11 bugs, certains jugés très graves.

Selon des chercheurs d'IBM X-Force , l'un des bugs les plus importants corrigés par Apple est une vulnérabilité d'escalade de privilèges affectant Apple iOS et iPadOS (jusqu'à 13,7). Traquée sous le nom de CVE-2020-9992, la vulnérabilité pourrait être exploitée si une cible était amenée à ouvrir un fichier spécialement conçu.

Les utilisateurs d'Apple doivent appliquer la mise à jour.

Consultez la source pour des informations supplémentaires sur les correctifs de sécurité Apple.

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

Actualité

De plus en plus d'attaques sur les infrastructures DNS

15 septembre 2020

Alors que les serveurs DNS ont longtemps été sous le radar des pirates informatiques, utilisés pour recherche d'informations d'entreprise et privées, les récentes attaques indiquent un changement d'approche et une situation qui nécessite une attention particulière […].

Plusieurs façons de lancer des attaques DNS :

- Les cybercriminels ciblent les routeurs et reconfigurent leurs paramètres DNS, dirigeant les victimes vers des sites Web malveillants au lieu des pages qu'ils ont l'intention de visiter.
- L'une des techniques implique l'utilisation de botnets pour cibler des serveurs avec des volumes massifs de requêtes DNS, inondant les serveurs de requêtes malveillantes et bloquant les requêtes légitimes.
- Les attaquants abusent souvent du DNS pour envahir un réseau privé, évitant ainsi la politique de même origine - un mécanisme qui permet à une page Web d'accéder aux données d'une autre page uniquement si les deux ont des noms d'hôte, des numéros de port et des numéros d'identification similaires.

Les fournisseurs de services DNS et les administrateurs peuvent empêcher de nombreuses attaques en suivant certaines mesures de sécurité recommandées. Dans le cadre de leurs opérations de sécurité, les organisations peuvent mettre en œuvre la surveillance des enregistrements DNS, utiliser des outils dédiés pour suivre les tentatives de piratage DNS, assurer une correction régulière des vulnérabilités et mettre en œuvre les extensions de sécurité du système de noms de domaine (DNSSEC) […].

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

Tendances des attaques réseau : les attaquants profitent de la gravité et de l'importance des exploits

15 septembre 2020

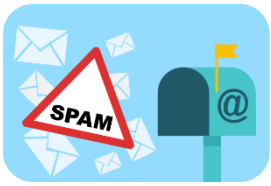
Du 1er mai au 21 juillet 2020, une équipe de chercheurs (Unite42) en cyber menaces ont capturé le trafic réseau mondial des pare-feu du monde entier, puis ont analysé les données pour examiner les dernières tendances des attaques réseau. La majorité des attaques observées ont été classées comme de sévérité élevée (56,7%), et près d'un quart (23%) ont été classées comme critiques. Les vulnérabilités les plus couramment exploitées sont CVE-2012-2311 et CVE-2012-1823 , toutes deux de type injection de commandes dans les scripts PHP CGI. Cela indique que les attaquants recherchent des exploits à fort impact […].

Les pays d'origine des attaques les plus actives sont la Chine, la Russie et les États-Unis. Bien que ces exploits remontent à huit ans (2012), certains exploits basés sur des vulnérabilités révélées cette année-là sont toujours actifs aujourd'hui car il reste possible de les exploiter. Cela souligne la nécessité pour les organisations de corriger rapidement et de mettre en œuvre les meilleures pratiques de sécurité notamment en terme de politique de mise à jour.

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

Les spammeurs utilisent des adresses IP hexadécimales pour éluder la détection

18 septembre 2020



Un groupe de spam a mis au point une astuce intelligente qui lui a permis de contourner les filtres de messagerie et les systèmes de sécurité et de parvenir dans un plus grand nombre de boîtes de réception que d'habitude.

Comme décrit dans la norme RFC79, les adresses IP peuvent également être écrites dans trois autres formats Octal, Hexadécimal, Integer / DWORD.

Selon un rapport publié par Trustwave, un groupe de spam a adopté des adresses IP hexadécimales pour ses campagnes depuis la mi-juillet plus tôt cette année.

Le groupe a envoyé des e-mails contenant des liens vers leurs sites de spam, mais au lieu de noms de domaine comme "spam-website.com", les e-mails contiennent des URL étranges telles que https:// 0xD83AC74E […].

Tout comme dans le rapport Trustwave, les opérations précédentes utilisaient ces étranges schémas d'adressage IP comme moyen de contourner la détection, car tous les logiciels de sécurité ne sont pas entièrement conformes à la RFC791.

Source : *https://zd.net/33TilFQ*

Les pirates mènent une guerre contre plus de 300000 sites WordPress vulnérables

10 septembre 2020

Des attaquants exploitant activement une faille critique d'exécution de code à distance affectant plus de 600000 sites WordPress, qui exécutent des versions de plugins vulnérables de File Manager, ont également été vus protéger les sites qu'ils compromettaient contre les attaques d'autres parties.

La vulnérabilité critique permet aux attaquants non authentifiés de télécharger des fichiers PHP malveillants et d'exécuter du code arbitraire après une exploitation réussie [1 , 2 , 3]. L'équipe de développement de File Manager a corrigé la faille avec la version File Manager 6.9 […].

Même si la faille a été corrigée quelques heures après que les développeurs ont été informés par le chercheur à l'origine de la découverte de la faille zero-day, plusieurs attaques étaient déjà

en cours. Les chercheurs de la société de sécurité WordPress Defiant ont repéré plus de 1,7 million de sites sondés par des pirates entre le 1er septembre et le 3 septembre […].

Il est recommandé d'utiliser un pare-feu applicatif Web pour corriger virtuellement les vulnérabilités connues jusqu'à ce qu'une mise à jour officielle est publiée.

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

Zeppelin Ransomware réapparaît comme une nouvelle menace pour le secteur de la santé

14 septembre 2020

Le secteur de la santé est déjà confronté à une pression énorme en termes de cybersécurité, et il a été l'un des secteurs clés les plus ciblés par les cybercriminels pendant la pandémie COVID-19.

Récemment, un ancien ransomware est réapparu avec de nouvelles vagues d'attaques contre les secteurs de la santé et de la technologie […].

La vague d'attaques est restée longtemps non détectée par les applications antivirus, en raison de l'utilisation par Zeppelin d'un nouveau téléchargeur de chevaux de Troie about1.vbs, caché dans le texte de poubelle des scripts Visual Basic […].

Pour faire face à ces menaces, il est recommandé aux organisations d'adopter une stratégie de cybersécurité à plusieurs niveaux et qu'elle soit proactive.

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

Android 11 : cinq nouvelles fonctionnalités de sécurité et de confidentialité à connaître

18 septembre 2020

Selon la dernière annonce de Google, le dernier système d'exploitation Android 11 comprend quelques nouvelles mesures intégrées conçues pour sécuriser les données des utilisateurs par défaut, augmenter la transparence et offrir un meilleur contrôle. Les fonctionnalités sont :

Autorisations uniques Permet aux utilisateurs d'accorder aux applications un accès à usage unique aux autorisations les plus sensibles de l'appareil, telles que l'emplacement, le microphone et la caméra.

Réinitialisation automatique des autorisations pour les applications inutilisées Permet au système d'exploitation mobile de réinitialiser automatiquement les autorisations d'exécution sensibles pour une application que l'utilisateur n'a pas utilisée depuis quelques mois.

Correctifs de sécurité rapides via les modules Play Store

Les utilisateurs d'Android 11 recevraient des correctifs de sécurité et de bug dès qu'ils seraient disponibles au lieu de compter sur les fabricants d'appareils pour publier des mises à jour au niveau du système d'exploitation.

Application du stockage étendu pour protéger les données

Les applications ne nécessitent aucune autorisation spéciale pour enregistrer et accéder à leurs propres fichiers sandbox sur le stockage externe. Cependant, si une application doit accéder ou modifier des fichiers créés par d'autres applications, elle doit d'abord demander l'autorisation appropriée.

Restreindre l'accès inutile aux emplacements en arrière-plan Lorsqu'une application demande l'autorisation d'accéder à votre emplacement, Android 11 garantit d'abord n'accorder que l'emplacement au premier plan, et si elle nécessite également l'accès à l'emplacement depuis l'arrière-plan, l'application doit faire une demande d'autorisation distincte.

C'était donc une brève introduction à toutes les fonctionnalités de sécurité et de confidentialité importantes disponibles pour les utilisateurs de smartphones dotés du dernier Android 11.

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

Le nouveau logiciel malveillant CDRThief vise à voler vos enregistrements de détails d'appels VoIP

11 septembre 2020

Récemment, un nouveau malware a été identifié ciblant les métadonnées critiques des appels Voice over IP (VoIP) stockées sur des serveurs Linux.

Une analyse plus approfondie des logiciels malveillants a révélé que les développeurs ont une connaissance approfondie du fonctionnement interne des produits ciblés. Pour voler des données, le malware interroge les bases de données MySQL utilisées par le softswitch, ce qui nécessite la connaissance des schémas de base de données internes […].

Le logiciel malveillant est capable de lire les fichiers de configuration qui stockent les mots de passe chiffrés pour la base de données MySQL intégrée, indiquant les compétences de ces pirates […].

Il est très sûr de dire que les attaquants continueront à déployer leurs efforts vers le développement de nouveaux outils et techniques pour altérer l'infrastructure basée sur les systèmes Linux pour un meilleur retour sur investissement. C'est certainement un sujet de préoccupation pour les entreprises qui comptent sur les systèmes Linux pour leur forte promesse de sécurité de type Unix.

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

Evènements

Evènements du mois

Conférence arabe sur la sécurité

Egypte, 06 - 12 Septembre 2020

https://bit.ly/3j2LNQa

Alors que la sécurité de l'information devient la plus grande préoccupation du monde d'aujourd'hui, Arab Security Consultants, société opérant dans le domaine de la sécurité de l'information en Egypte et au Moyen-Orient, a décidé de réunir les plus grandes personnalités du domaine localement et mondialement ainsi que les principaux PDG de grandes entreprises en un seul endroit.

Dans sa quatrième édition, plus de 500 participants des communautés opérationnelles, gouvernementales, commerciales et techniques de la cybersécurité ont participé à cette conférence.

Voici les principaux points qui ont été abordées durant cet évènement :

- La Conférence arabe sur la sécurité a aidé les participants à rester au fait des dernières tendances en matière de cybersécurité et à établir de nouvelles relations avec des professionnels du monde entier.
- Aller au-delà de la recherche de solutions et explorer les menaces de cybersécurité.
- Plus de 30 ateliers et sessions traitant de nouvelles pistes axées sur la cyber menace.
- Créer un réseau avec des professionnels et des pairs du monde entier à tous les niveaux tout au long de la conférence.
- Découvrir une opportunité unique afin d'acquérir des compétences pratiques dans les domaines dynamiques de la cybersécurité et de la sécurité de l'information.

Hack at the Harbour, virtuel

25 septembre 2020

https://bit.ly/3396zbv

Hack at the Harbor est une conférence virtuelle nouvellement développée créée par les fondateurs de Point3 Security.

Hack at the Harbor a été conçue par et pour les professionnels de la sécurité, pour responsabiliser les équipes de sécurité et les environnements de travail, et pour aider les professionnels de la sécurité à faire progresser leurs objectifs de carrière.

Les sessions ont fourni aux participants des informations exploitables et des opportunités de renforcement des compétences, en se concentrant sur des sujets, tels que :

- Les nouveaux risques et attaques, en identifiant et en comblant les lacunes de compétences critiques, en renforçant l'équipe, en soutenant le personnel de sécurité, en communiquant entre les départements autour de la sécurité,
- Le soutien de la santé mentale, la mise en place d'objectifs de diversité et d'inclusion mise en pratique,
- Les tendances en matière de sécurité et la formation des équipes.

Evènements à venir

EuroCACS 2020, Virtuel

28 - 30 Octobre 2020

https://bit.ly/3j9aevg

EuroCACS 2020 Virtual rassemble 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.

Les sessions virtuelles EuroCACS 2020 sont destinées aux professionnels à tout moment de leur carrière. Avec trois niveaux d'apprentissage, une formation technique et des compétences générales, des conférences, des tables rondes et plus encore.

Reference	ANPT-2020-BV-09
Titre	Bulletin de veille N°9
Date de version	30 Septembre 2020
Contact	ssi@anpt.dz