BULLETIN DE VEILLE N°1

ANPT-2019-BV-01

« L'homme et sa sécurité doivent constituer la première préoccupation de toute aventure technologique. » - Albert Einstein -

Mai 2019

Alertes de sécurité

Microsoft

Vulnérabilité dans Microsoft Remote Desktop Services (RPC)

14 mai 2019

Microsoft a publié un correctif pour une vulnérabilité identifiée comme CVE-2019-0708. Cette Vulnérabilité impacte les services de bureau à distance basé sur le protocole RDP. La vulnérabilité permet l'exécution de code arbitraire sur un système vulnérable sans authentification ni interaction d'un utilisateur.

Systèmes affectés : Windows 7, Server 2008 R2, Server 2008, Vista, 2003 et XP

Pour éviter l'exploitation de cette vulnérabilité en pré-authentification, il est recommandé d'utiliser la fonctionnalité **NLA** qui force une authentification du client lors de la connexion RDP. Il est aussi recommandé d'appliquer les **correctifs disponibles** dans les plus brefs délais.

Source : *https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-006/*
Détails CVE : *https://nvd.nist.gov/vuln/detail/CVE-2019-0708*

Vulnérabilité dans le serveur DHCP de Windows

16 mai 2019

Microsoft a publié un correctif pour une vulnérabilité identifiée comme CVE-2019-0725, cette vulnérabilité permet à un attaquant, non authentifié, d'exécuter du code arbitraire à distance après avoir envoyé un paquet spécialement conçu au serveur DHCP [...].

Systèmes affectés : Windows Server 2008 R2 SP1, 2012, 2012 R2, 2016 et 2019

Source : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0725
Détails CVE : https://nvd.nist.gov/vuln/detail/CVE-2019-0725

Oracle

Vulnérabilité dans Oracle WebLogic

02 mai 2019

Une vulnérabilité dans les composants d'Oracle WebLogic Server et Oracle Fusion Middleware identifiée comme CVE-2019-2725 permet l'exécution de commande à distance et ainsi compromettre le serveur vulnérable.

Versions affectées : WebLogic Server v10.3.6.0.0 et v12.1.3.0.0

Un module Metasploit exploitant cette vulnérabilité a été publié sur Exploit-db le 08 mai 2019

Il est recommandé de se référer au site officiel de l'éditeur pour l'application des correctifs.

Source : *https://www.cert.ssi.gouv.fr/alerte/CERTFR-2019-ALE-005/*
Détails CVE : *https://nvd.nist.gov/vuln/detail/CVE-2019-2725*
Exploit : *https://www.exploit-db.com/exploits/46814*
Patch : *https://www.oracle.com/technetwork/security-advisory/alert-cve-2019-2725-5466295.html*

Cisco

Des vulnérabilités dans les commutateurs Nexus

02 mai 2019

Cisco a émis une quarantaine d'avis de sécurité, dont un avis « critique » concernant une vulnérabilité dans le logiciel du commutateur de datacenter Cisco Nexus 9000. La faille concerne un problème de gestion des clés SSH qui permettrait à un attaquant distant de se connecter au système affecté avec des privilèges d'un root. Elle n'est exploitable que sur IPv4, IPv6 n'étant pas impacté par cette vulnérabilité.

Source : *http://www.reseaux-telecoms.net/actualites/lire-cisco-emet-un-avis-de-securite-critique-pour-les-commutateurs-de-datacenter-nexus-9000-27745.html*

Google

BUFFER OVERFLOW

23 mai 2019

Une vulnérabilité affectant le composant Skia du navigateur web Google Chrome a été publiée, identifiée par CVE-2019-5798 et classée critique. Elle permet à un attaquant distant de réaliser un buffer overflow via une page HTML craftée.

Il est recommandé de mettre à jour le navigateur en sa version la plus récente qui a patché cette faille.

Source : *https://vuldb.com/fr/?id.135476*
Détails CVE : *https://nvd.nist.gov/vuln/detail/CVE-2019-5798*

ELÉVATION DE PRIVILÈGES

23 mai 2019

Une vulnérabilité affectant le composant Blink du moteur de recherche Google Chrome identifiée comme CVE-2019-5800 et classée critique permettrait à un attaquant distant de perpétrer une attaque de type escale de privilèges.

Il est recommandé de mettre à jour à la version 73.0.3683.75 qui élimine cette vulnérabilité.

Source : *https://vuldb.com/fr/?id.135478*
Détails CVE : *https://nvd.nist.gov/vuln/detail/CVE-2019-5800*

Mozilla

Multiples vulnérabilités dans Mozilla Firefox et Thunderbird

23 mai 2019

De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service et un contournement de la politique de sécurité.

Ces vulnérabilités correspondent au CVE suivants : *CVE-2019-9815*, *CVE-2019-9816*, *CVE-2019-9817*, *CVE-2019-9818*, *CVE-2019-9819*, *CVE-2019-9820*, *CVE-2019-11691*, *CVE-2019-11692*, *CVE-2019-11693*, *CVE-2019-7317*, *CVE-2019-9797*, *CVE-2018-18511*, *CVE-2019-11694*, *CVE-2019-11698*, *CVE-2019-5798*, *CVE-2019-9800*, CVE-2019-9821, CVE-2019-11695, CVE-2019-11696, CVE-2019-11697, CVE-2019-11700, CVE-2019-11699, CVE-2019-11701, CVE-2019-9814

Il est recommandé de mettre à jour Mozilla Thunderbird à la version 60.7 et Firefox à la version 67.

Source : https://www.mozilla.org/en-US/security/advisories/mfsa2019-15 https://www.mozilla.org/en-US/security/advisories/mfsa2019-13/

Actualité

Des mots de passe G Suite étaient stockés en clair chez Google depuis 2005

21 mai 2019

Google a révélé que les mots de passe de plusieurs de ses clients travaillant sur G Suite avaient été stockés en texte clair sur des systèmes internes (unhashed). Cette vulnérabilité n'affecte que les comptes professionnels, les comptes gratuits ne sont pas affectés [...].

G suite est un outil destiné aux professionnels pour les applications Google. Dans le passé, l'administrateur pouvait définir le mot de passe d'un employé qui était stocké dans un fichier texte non crypté. C'est cette faible protection qui a été découverte récemment par les clients et corrigée par Google.

Source : *https://cloud.google.com/blog/products/g-suite/notifying-administrators-about-unhashed-password-storage [Originale : ANG]*

La sécurité des routeurs Cisco ISR/ASR SD-WAN se renforce

09 mai 2019

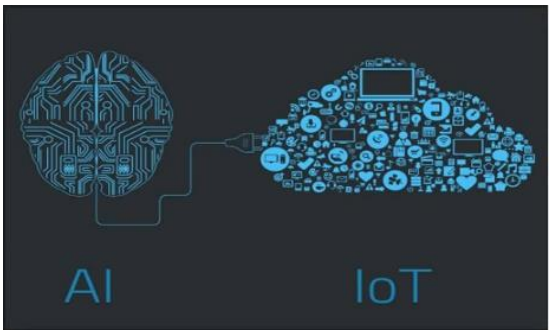
Cisco a ajouté la prise en charge d'AMP (Advanced Malware Protection) à ses millions de routeurs périphériques ISR / ASR, dans le but de renforcer la protection contre les programmes malveillants des succursales et des réseaux centraux au niveau du réseau SD-WAN [...].

Le support AMP vient renforcer une panoplie conséquente de fonctions de sécurité déjà comprises dans le logiciel SD-WAN, comme le filtrage d'URL, la sécurité DNS Umbrella, la prévention des intrusions Snort Intrusion Prevention, la possibilité de segmenter les utilisateurs à travers le WAN et une sécurité intégrée de la plate-forme, notamment le module Trust Anchor.

Source : *https://www.networkworld.com/article/3394597/cisco-adds-amp-to-sd-wan-for-israsr-routers.html [originale : ANG]*

De l'IoT à l'AIoT pour la sécurité d'Internet des objets

26 mai 2019



Extreme Networks a lancé son application ExtremeAI Security, une solution de sécurité réseau qui tire parti de l'intelligence artificielle et de l'apprentissage automatique pour identifier et résoudre les menaces avancées qui pèsent sur les appareils IoT.

La convergence du multi-cloud, de la mobilité et de l'afflux massif de périphériques IoT dans l'entreprise élargit la surface d'attaque, ce qui impose de déployer des technologies de sécurité avancées au cœur du réseau et pas seulement au périmètre, a déclaré Externe Networks. Cette **explosion de points de terminaison et de trafic réseau** créerait de la complexité et empêcherait les administrateurs de réseau et les équipes de sécurité d'obtenir une visibilité sur le chaos par le biais de solutions traditionnelles [...].

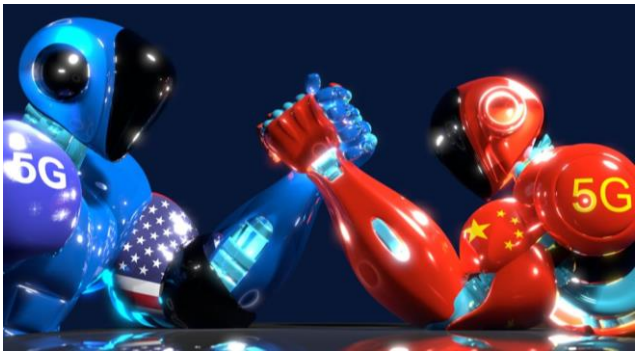
ExtremeAI Security offre une visibilité et une détection approfondies du trafic malveillant, ainsi qu'une surveillance en temps réel des périphériques IoT pour détecter les anomalies comportementales.

Les fonctionnalités d'analyse de trafic et de visibilité d'Extreme sont intégrées à cette nouvelle solution de sécurité, associant la mise en réseau d'entreprise aux innovations en matière d'apprentissage automatique afin d'identifier et de résoudre les menaces. La solution sera disponible en octobre 2019.

Source *: https://hostingjournalist.com/cybersecurity/extreme-networks-unveils-iot-security-and-automated-threat-mitigation-extremeai-security/*

La guerre pour la 5G !!

28 mai 2019



Les États-Unis, la Chine et l'Union Européenne se livrent actuellement une guerre secrète pour être le premier à créer son réseau 5G. Il faut dire que les enjeux économiques et industriels sont énormes.

La guerre pour la 5G a commencé. Ce réseau mobile ultra-rapide est considéré par les États-Unis comme une « priorité pour la défense nationale », ainsi que pour l'économie américaine – au point qu'en mai 2018, Donald Trump a affirmé sa volonté de construire au plus vite un « réseau national centralisé », visant 2019 comme deadline.

Il faut dire que face aux USA, se dresse une nouvelle grande puissance, qui selon une étude aurait « une longueur d'avance » sur ses concurrents occidentaux : la Chine [...]. Des entreprises comme Huawei et ZTE développent déjà des smartphones capables de télécharger à la vitesse de 10 Gigabits par seconde (vitesse promise par la 5G) – et sont donc en avance sur leurs concurrents. Des opérateurs comme China Mobile seraient en outre prêts à déployer le réseau mobile nouvelle génération avant la fin de l'année 2018.

Face à la « menace » que représente la Chine, Donald Trump a signé un décret visant à limiter la vente d'appareils mobiles chinois sur le territoire US.
Pourquoi la 5G semble-t-elle être à ce point un enjeu stratégique et commercial ? Avec le débit ultra rapide qu'elle annonce (un réseau 100 fois plus rapide que les réseaux 4G actuels), la 5G porte en elle la promesse d'un véritable bond technologique. Grâce à une connexion décuplée et à une latence presque inexistante, permettant aux utilisateurs d'être connectés en permanence, ce « réseau mobile du futur » devrait en effet permettre de mieux gérer les voitures autonomes, de créer des jeux vidéo en VR, de développer toujours plus l'Internet des objets ainsi que l'industrie du streaming, ou encore la chirurgie virtuelle…[…] Selon un rapport récent de l'Arcep (Autorité de Régulation des Communications Electroniques et des Postes française), la 5G et son débit ultra-rapide permettront finalement de « numériser réellement la société et l'économie » (en premier lieu les entreprises) – et donc de nous propulser enfin vers le futur.

Cela augmentera en contrepartie les risques et les vulnérabilités qui menacent la sécurité des appareils connectés et du flux de plus en plus important qui est généré.

Source : https://www.outthere.fr/briefs/pourquoi-la-5g-est-elle-un-enjeu-strategique-pour-les-grandes-puissances

Evènements

Evènements du mois

Hack In The Box Conference

6-10 mai 2019. Amsterdam, Pays-Bas

https://conference.hitb.org

La conférence sur la sécurité Hack In The Box est mondialement reconnue pour ses possibilités de mise en réseau et ses idées novatrices sur les questions de sécurité informatique. Elle est organisée chaque année à Amsterdam et traite des thèmes et des idées novatrices sur les questions de sécurité informatique. Des conférences, des workshops et des challenges sont programmées chaque année sur des sujets tels que : l'apprentissage automatique, sécurité des IoT, cryptographie…et autres.

International Cryptographic Module Conference

14- 17 mai 2019.Vancouver, Canada

https://icmconference.org

L'événement annuel le plus important pour l'expertise mondiale en cryptographie commerciale. Plus de 25 pays se sont réunit pour discuter des défis uniques auxquels font face ceux qui développent, produisent, testent, spécifient et utilisent des modules cryptographiques, en mettant l'accent sur des normes telles que FIPS 140-2, ISO/IEC 19790 et Critères communs.

Evènements à venir

Infosecurity Europe 2019

4 juin 2019. Londres, Royaume-Uni

Site web:

https://www.infosecurityeurope.com

Gartner Security & Risk Management Summit 2019

17-20 juin 2019. Oxon Hill, États-Unis

Site web :

https://www.gartner.com/en/conferences/

Reference	ANPT-2019-BV-01
Titre	Bulletin de veille N°1
Date de version	29 Mai 2019
Contact	ssi@anpt.dz