REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

Bulletin de sécurité N°2 du mois d'Octobre 2018

B.P. 6170 Tél : 22 08 64 98 Fax : 22 20 39 29 Web : http//www.antic.cm ; Email : infos@antic.cm

Sommaire

I. LEXIQUE DU BULLETIN

Expression	Signification
Date de publication	Date à laquelle la vulnérabilité a été officiellement publiée par le développeur ou constructeur de la ressource concernée.
Dernière version	Lien de téléchargement de la dernière version de la ressource concernée, dans le cas d'une ressource logicielle ou système d'exploitation.
Description	Présentation des détails sur la vulnérabilité, entre autre les versions de la ressource concernée par la vulnérabilité, le vecteur d'exploitation de la vulnérabilité (local, réseau …).
Référence CVE	CVE (Common Vulnerabilities and Exposures) est un annuaire de vulnérabilités de sécurité. Cet annuaire est maintenu par l'organisme MITRE, soutenu par le Département de la Sécurité intérieure des États-Unis. Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro incrémenté). Plus d'information à l'adresse : http://cve.mitre.org/
Score CVSS	CVSS (Common Vulnerability Scoring System) est un système d'évaluation des vulnérabilités qui permet d'associer une valeur (comprise entre 0 et 10) évaluant la criticité d'une vulnérabilité. CVSS fournit un cadre commun pour évaluer les niveaux de criticité, les caractéristiques et les impacts des vulnérabilités de sécurité informatique. Plus d'informations à aux adresses : http://www.first.org/cvss/cvss-guide.html, http://www.cert-ist.com/fra/ressources/Publications_ArticlesBulletins/Veilletechnologique/CVSSv2/
Solution	Lien vers d'éventuelles solutions permettant de colmater ou de contourner la vulnérabilité.
Vulnérabilité	Faille de sécurité publiée, Synopsis de la faille, généralement sur la forme « Vulnérabilité dans X » où X est une ressource informatique, matérielle, logicielle ou système d'exploitation concernée par la vulnérabilité.

II. Vulnérabilités publiées

II.1 Navigateurs

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Firefox et Mozilla Firefox ESR	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et un déni de service. Les versions concernées sont les suivantes : Mozilla Firefox de versions antérieures à la version 63. Mozilla Firefox ESR de versions antérieures à la version 63.3	24/10/2018	CVE-2018-12403	63 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Google Chrome	Google a publié la version 70.0.3538.67 de Google Chrome pour Windows, Mac et Linux. Cette version corrige des vulnérabilités qu'un attaquant pourrait exploiter pour prendre le contrôle d'un système affecté. Les systèmes affectés sont les suivants : Google Chrome version antérieure à 70.0.3538.76	17/10/2018	CVE-2018-17477	70.0.3538.77 Télécharger	Effectuez une mise à jour du navigateur	10.0

II.2 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Plusieurs vulnérabilités ont été corrigées dans le CMS Drupal. Une exploitation réussie de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : Drupal Core versions 8.6.x antérieures à 8.6.2	18/10/2018	CVE-2018-17859	8.6.2 Télécharger	Mettre à jour le CMS	10.0

II.3 SYSTÈMES D' EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	Une critique vulnérabilité de type Zero-Day a été découverte dans Microsoft Data Sharing (dssvc.dll). Cette vulnérabilité affecte uniquement les versions récentes du système d'exploitation Windows, telles que Windows 10 (toutes les versions, y compris la dernière mise à jour d'octobre 2018) et Server 2016, puisque le service Microsoft Data Sharing (dssvc.dll) n'est pas présent sur les systèmes Windows 8.1 et antérieurs. Un exploit réussi de cette faille permet à un attaquant ayant accès au système de réussir une élévation de privilèges. Un Proof Of Concept a été récemment publié. Il était codé en particulier pour supprimer les fichiers pour lesquels un utilisateur aurait normalement besoin de privilèges d'administrateur pour le faire. **Solution :** En attendant le patch de Microsoft, il est recommandé d'évaluer le risque de cette faille sur votre SI et de prendre les mesures nécessaires pour atténuer ce risque.					10.0
Vulnérabilité dans les produits Microsoft	Microsoft a publié une mise à jour de sécurité pour corriger une vulnérabilité dans Yammer desktop application. Un attaquant distant pourrait exploiter cette vulnérabilité pour prendre le contrôle d'un système affecté.	19/10/2018	CVE-2018-8569	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans le noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Elles permettent à un attaquant de provoquer un déni de service et une atteinte à la confidentialité des données.	26/10/2018	CVE-2017-14633	4.18.16 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20183470-1/	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits IBM	Une vulnérabilité a été corrigée dans IBM Security Access Manager appliance. L'exploitation de cette faille pourrait permettre à un attaquant d'exécuter des opérations non autorisées lorsque les services Advanced Access Control sont en cours d'exécution. Les versions affectées sont les suivants : IBM Security Access Manager 9.0.3.1, 9.0.4.0, 9.0.5.0	23/10/2018	CVE-2018-1850	9.0.5.0 Contacter IBM	Effectuez une mise à jour du système	2.1
Vulnérabilité dans les produits VMware	Une vulnérabilité a été corrigée dans VMware ESXi, Workstation et Fusion. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code à distance et de prendre le contrôle du système affecté. Les systèmes infectés sont les suivants : • VMware vSphere ESXi (ESXi) 6.7 • VMware Workstation Pro / Player (Workstation) 14.1.3 • VMware Fusion Pro, Fusion (Fusion)10.1.3	17/10/2018	CVE-2018-6974	Contacter VMware	Effectuez une mise à jour	4.2

Vulnérabilité dans HP iLO	Une vulnérabilité a été découverte dans HP iLO. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • HPE Integrated Lights-Out 5;	25/10/2018	CVE-2018-7105	Contacter HP	Contacter HPE pour une mise à jour du firmware	4.5
Vulnérabilité dans les produits CISCO	Plusieurs vulnérabilités ont été corrigées dans plusieurs produits Cisco. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code à distance, de prendre le contrôle du système affecté, de causer un déni de service, de réussir une élévation de privilèges et d'accéder aux informations confidentielles.	18/10/2018	CVE-2018-15435	Contacter Cisco	Veuillez-vous référer au guide de sécurité de CISCO pour obtenir les correctifs • https://tools.cisco.com/security/center/publicationListing.x	7.8

Vulnérabilité dans X.Org	Une faille a été trouvée dans xorg-x11-server de version antérieure à 1.20.3. Un contrôle d'autorisation incorrect pour les options -modulepath et -logfile lors du démarrage de Xorg X server permet aux utilisateurs non privilégiés ayant la possibilité de se connecter au système via une console physique, d'élever leurs privilèges et d'exécuter du code arbitraire sous les privilèges root.	25/10/2018	CVE-2018-14665	7.7 Télécharger	Mettre à jour le serveur	-
Vulnérabilité dans les routeurs Linksys E Series	Plusieurs vulnérabilités ont été corrigées dans la gamme de routeurs Linksys E Series. Une exploitation réussie de ces vulnérabilités via des requêtes spécialement conçues pour la configuration du réseau pourrait permettre à des attaquants d'exécuter du code arbitraire.	18/10/2018	CVE-2018-3955	Contacter Linksys	Veuillez-vous référer au guide de sécurité de Linksys pour obtenir les correctifs. https://www.talosintelligence.com/reports/TALOS-2018-0625	7.2
Vulnérabilité dans SYmantec	Une vulnérabilité a été corrigée dans Symantec Web Isolation. L'exploitation de cette faille permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Le système infecté est le suivant : Symantec Web Isolation (WI) versions 1.11.x antérieures à 1.11.21.	18/10/2018	CVE-2018-12246	Contacter Symantec	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://support.symantec.com/content/unifiedweb/en_US/article.SYMSA1464.html	6.1

III. ACTUALITÉS

1. Windows defender premier antivirus…….

Ceux qui pensent encore que l'antivirus de Windows est à la traîne par rapport aux autres vont devoir changer d'avis, et rapidement. Depuis l'arrivée de Windows 10, les développeurs de Microsoft ont fourni un travail exemplaire pour enrichir leur solution de sécurité et la mettre au même niveau que les autres solutions du secteur.

https://www.01net.com/actualites/windows-defender-premier-antivirus-a-s-executer-dans-un-bac-a-sable-1554740.html

2. Espionnage : iPhone pour Huawei

Il y a quelques jours, The New York Times a révélé que Donald Trump se faisait régulièrement espionner par la Chine et la Russie lorsqu'il passe des coups de fil avec ses iPhone. Selon le journal, le président des Etats-Unis dispose en effet de trois smartphones. Deux sont officiels et ont été durcis par la NSA. L'un est utilisé pour Twitter, l'autre pour les conversations téléphoniques. Mais Donald Trump possèderait également un troisième iPhone, strictement personnel et non sécurisé.

https://www.01net.com/actualites/espionnage-la-chine-recommande-a-donald-trump-de-lacher-son-iphone-pour-un-huawei-1552661.html

3. Effacez les données de recherches Google en deux clics

Finis les menus abscons et introuvables. Google vient de simplifier l'accès aux réglages de confidentialité et de sécurité depuis son produit phare, la recherche en ligne. Désormais, si vous allez sur Google.com ou Google.fr et que vous êtes connecté, vous verrez un lien directement sous la barre de recherche.

https://www.01net.com/actualites/desormais-effacez-vos-donnees-de-recherche-google-en-deux-clics-1551602.html

4. Mozilla veut utiliser firefox pour vendre des services VPN

Avec un VPN, les opérateurs de boucle locale ne pourront pas non plus savoir quelles sont vos habitudes de surf, une information qui les intéresse de plus en plus. Par ailleurs, un service VPN ajoute une couche de chiffrement sur les données échangées, apportant une sécurité supplémentaire dans certains endroits où la sécurité n'est pas exceptionnelle (cafés, hotels, aéroports…).

https://www.01net.com/actualites/mozilla-veut-utiliser-firefox-pour-revendre-des-services-vpn-1550048.html

5. 21 ans de prison pour avoir vendu un malware

Aujourd'hui âgé de 21 ans, Colton Grubbs a conçu le logiciel LuminosityLink alors qu'il était encore adolescent. D'après ses premières déclarations, il ne s'agissait à la base que d'un outil destiné aux administrateurs système, sans intention malveillante. Mais en juillet 2017, il a finalement admis que son programme était utilisé comme un cheval de Troie administré à distance (« RAT » en anglais) et qu'il avait lui-même mis en avant des fonctionnalités illégales. Parmi celles-ci, la possibilité d'enregistrer les touches utilisées sur le clavier de la victime, de contrôler sa webcam et son micro, de voler des mots de passe, de miner de la cryptomonnaie à son insu, etc.

https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/malware-logiciel-malveillant/actualite-846445-30-prison-vendu-logiciel-malveillant.html

6. Une faille de sécurité qui exploite l'intégration de vidéo

L'équipe de recherche de Cymulate a découvert un moyen d'abuser de la fonction Vidéo en ligne sur Microsoft Word pour exécuter un code malveillant. Cette technique permet d'infecter un ordinateur via des documents Word sans déclencher un avertissement de sécurité révélateur en exploitant une fonctionnalité qui, à la base, permet d'intégrer directement des vidéos dans des fichiers Word.

https://www.developpez.com/actu/231242/Une-faille-de-securite-exploitant-la-fonction-d-integration-de-video-en-ligne-sur-Microsoft-Word-permet-d-executer-aisement-un-code-malveillant/

7. Chine et USA principales sources cyberattaques

NSFocus, une entreprise spécialisée dans la sécurité informatique, a publié une étude complète portant sur l'analyse du trafic internet entre le 1er janvier et le 30 juin 2018. Les résultats listent point par point les différents types d'attaques informatiques et leur volume. La société a recensé près de 27 millions d'attaques informatiques durant ces six premiers mois de l'année. 40% d'entre elles ont été réalisées par des hackers « récidivistes », qui représentent 25% des pirates identifiés. Ces derniers se situent en Chine, aux Etats-Unis et en Russie. Selon l'étude, les hackers réutilisent régulièrement leurs techniques et renouvellent peu leurs méthodes de piratage.

https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-846579-chine-etats-unis-principales-sources-cyberattaques-premier-semestre-2018.html

IV. NOTES IMPORTANTES

1. Veuillez enregistrer les adresses alerts@antic.cm et alerts@cirt.cm parmi vos contacts ou l'enregistrer comme expéditeur approuvé afin de ne plus recevoir les mails en provenance de cette adresse dans vos spam.
2. Ce document est produit régulièrement et téléchargeable sur notre site web www.cirt.cm . Vous y trouverez aussi des alertes et autres publications relatives à la cybersécurité et à la cybercriminalité.
3. Windows XP SP3 et Office 2003 ne sont plus supportés depuis le 8 avril 2014 par Microsoft. Si votre organisation n'a pas encore effectué une migration vers un poste de travail moderne, votre système d'information court de grands risques. En se basant sur les données des déploiements passés des clients Microsoft, le déploiement moyen en entreprise peut prendre de 18 à 32 mois. Pour plus d'informations :
   http://www.microsoft.com/fr-fr/windows/enterprise/fin-support-XP/default.aspx

   L'utilisation des solutions ne possédant aucun support technique présente un risque élevé étant donné qu'aucun correctif ne sera émis après d'éventuelles vulnérabilités détectées sur celles-ci.
4. HIDDEN COBRA - Cyberactivités nord-coréennes malveillantes : Le Département de la Sécurité Intérieure (DHS) et le Bureau Fédéral d'Investigation (FBI) ont identifié des activités malveillantes imputées au groupe dénommé HIDDEN COBRA, et ont fourni des détails techniques sur les outils et l'infrastructure utilisés par ces cyber-acteurs du gouvernement nord-coréen. Le but du partage de cette information est de sensibiliser les responsables des Systèmes d'Information sur la possibilité d'infection, et de réduire l'exposition à cette cyberactivité du gouvernement nord-coréen. Les outils de détection, et des solutions de prévention et d'éradication sont contenues dans les articles contenus dans la page suivante :
   https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity
5. Afin de se prémunir au maximum d'éventuelle attaques informatiques pouvant endommager tout ou partie de vos systèmes, vous devez mettre à jour tous vos systèmes et logiciels utilisés. Nous vous recommandons donc de télécharger et d'installer toutes les dernières versions de logiciels et systèmes utilisés, uniquement sur les sites des constructeurs. Car tout logiciel téléchargé d'une source autre que celle du constructeur est potentiellement compromise par des malware et chevaux de Troie.

   Par ailleurs, si vous rencontrez quelques difficultés que ce soit dans l'application des correctifs susmentionnés ou ailleurs vous pouvez nous contacter à travers les adresses email alerts@antic.cm et alerts@cirt.cm ou au numéro de téléphone **242 09 91 64**.