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°1 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	Mozilla Foundation annonce la disponibilité d'une mise à jour de sécurité permettant la correction de deux vulnérabilités critiques dans Mozilla Firefox et Mozilla Firefox ESR. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire. Les versions concernées sont les suivantes : Mozilla Firefox de versions antérieures à la version 62.0.3 Mozilla Firefox ESR de versions antérieures à la version 60.2.2	03/10/2018	CVE-2018-12387	62.0.3 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Edge	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une exécution de code à distance et un contournement de la fonctionnalité de sécurité. Les systèmes affectés sont les suivants : Microsoft Edge et Azure IoT Edge	10/10/2018	CVE-2018-8530	11 Télécharger	Effectuez une mise à jour du navigateur via Windows Update	10.0

Vulnérabilité dans Internet Explorer	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une exécution de code à distance.	10/10/2018	CVE-2018-8491	11 Télécharger	Effectuez une mise à jour du système via Windows Update	10.0

II.2 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Joomla	De multiples vulnérabilités ont été découvertes dans Joomla. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, un contournement de la politique de sécurité et une injection de requêtes illégitimes par rebond (CSRF). La version affectée est la suivante : Joomla de version antérieure à 3.8.13	10/10/2018	CVE-2018-17859	3.8.13 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	Plusieurs vulnérabilités ont été corrigées dans Microsoft Windows. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités afin de provoquer un déni de service, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et un contournement de la politique de sécurité.	10/10/2018	CVE-2018-8513	Windows 10	Mettre à jour le système via Windows UPDATE	10.0
Vulnérabilité dans les produits Microsoft	Plusieurs vulnérabilités ont été corrigées dans certains produits Microsoft. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités afin de provoquer une exécution de code à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Hub Device Client SDK for Azure IoT • ChakraCore • Azure IoT Edge	10/10/2018	CVE-2018-8531	-	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. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et d'avoir d'autres impacts de sécurité non spécifiés par l'éditeur.	10/10/2018	CVE-2017-17182	4.18.13 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20183084-1/	10.0
Vulnérabilité dans Apple iOS	Apple annonce la correction de plusieurs vulnérabilités dans son système d'exploitation pour téléphones iOS. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'accéder à des données confidentielles. Les systèmes affectés sont les suivants : Apple iOS de versions antérieures à la version 12.0.1	09/10/2018	CVE-2018-4380	12.0.1 Contacter Apple	Effectuez une mise à jour du système	4.2
Vulnérabilité dans OS Google Android	Google annonce la disponibilité d'une mise à jour de sécurité permettant la correction de plusieurs vulnérabilités au niveau de son OS Google Android. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder aux informations confidentielles, de réussir une élévation des privilèges et de causer un déni de service.	03/10/2018	CVE-2018-9515	9 (Pie)	Effectuez une mise à jour du système	7.3

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	Une vulnérabilité a été corrigée dans Microsoft .Net. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivants : NET Core 2.1.	10/10/2018	CVE-2018-8292	2.1 Télécharger	Effectuez une mise à jour du système via Windows Update	2.1
Vulnérabilité dans les produits VMware	Plusieurs vulnérabilités ont été corrigées dans certains produits VMware. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités afin de provoquer un déni de service. Les systèmes infectés sont les suivants : • VMware vSphere ESXi (ESXi) • VMware Workstation Pro / Player (Workstation) • VMware Fusion Pro, Fusion (Fusion)	10/10/2018	CVE-2018-6977	Contacter VMware	Effectuez une mise à jour	4.2

Vulnérabilité dans les produits Adobe	Adobe a publié des mises à jour qui permettent de corriger des vulnérabilités dans certains produits Adobe. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire, d'accéder à des informations confidentielles ou une élévation de privilèges. Les systèmes affectés sont les suivants : • Adobe Digital Edition version 4.5.8 et versions antérieures sur Windows, MacOS et iOS ; • Adobe Framemaker version 1.0.5.1 et versions antérieures sur Windows ; • Adobe Technical Communications Suite version 1.0.5.1 et versions antérieures sur Windows.	10/10/2018	CVE-2018-12823	Contacter Adobe	Installer les mises à jour	8.5

Vulnérabilité dans les produits CISCO	Cisco annonce la disponibilité d'une mise à jour de sécurité permettant la correction de plusieurs vulnérabilités au niveau de certains de ses produits. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder aux informations confidentielles, de réussir une élévation des privilèges et de causer un déni de service.	04/10/2018	CVE-2018-15334	Contacter Cisco	Veuillez-vous référer au guide de sécurité de CISCO pour obtenir les correctifs • https://tools.cisco.com/security/center/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities	7.8
Vulnérabilité dans D-Link Central WiFi Manager	Plusieurs vulnérabilités ont été corrigées dans D-Link Central WiFi Manager. Un attaquant pourrait exploiter ces vulnérabilités afin d'exécuter du code arbitraire à distance. Les systèmes affectés sont les suivants : D-Link Central WiFi Manager 1.03 et versions antérieures pour Windows.	05/10/2018	CVE-2018-17443	Contacter D_Link	Veuillez-vous référer au guide de sécurité de dlink pour obtenir les correctifs. https://securityadvisories.dlink.com/announcement/publication.aspx?name=SAP10092	7.2

Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une élévation de privilèges et une exécution de code à distance	10/10/2018	CVE-2018-8518	Contacter Microsoft	Effectuez une mise à jour du système via Windows Update	7.1

III. ACTUALITÉS

1. Des puces d'espionnage chinoises dans des prises Ethernet

Les journalistes de Bloomberg récidivent, après avoir évoqué la présence prétendue de puces d'espionnage dans les cartes mères de Supermicro, ajoutent une nouvelle couche à leur enquête. Dans un article publié le 9 octobre, ils expliquent qu'un « opérateur télécoms américain majeur » a récemment détecté une prise Ethernet vérolée sur une carte mère de Supermicro, intégrée dans un serveur.

https://www.01net.com/actualites/big-hack-des-puces-d-espionnage-chinoises-trouvees-dans-des-prises-ethernet-verolees-1541377.html

2. Le clickjaking nouveau fléau des internautes

Le clickjacking est une nouvelle technique visant à piéger des internautes non avertis. S'ajoutant ainsi au phishing , au cryptojacking, au credential stuffing et autres arnaques du web, le clickjacking (« détournement de clic ») est une attaque – passive mais pas moins vicieuse – qui profite d'une vulnérabilité présente dans des navigateurs web et permet à des individus malveillants de modifier l'apparence d'un site pour l'utilisateur, sans en changer le fonctionnement.

https://www.undernews.fr/reseau-securite/le-clickjacking-nouveau-fleau-des-internautes.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+undernews%2FoCmA+%28UnderNews%29

3. Liste des méthodes des pirates

Les pirates informatique et autres cybercriminels ne manquent pas d'imagination pour s'attaquer à leurs cibles. Voici le top des techniques utilisées ainsi que des conseils pour s'en protéger.

https://www.undernews.fr/fiches-pirates/techniques-de-pirates-liste-des-methodes-les-plus-courantes

4. Google + une faille de sécurité provoque sa fermeture

Google vient d'annoncer la fermeture de Google+. Certains le regretteront, d'autres seront surpris d'apprendre que Google+ existait encore en 2018. Pendant 7 ans, Google aura tenté, tant bien que mal, de développer son réseau social. La firme de Mountain View reconnaît son échec en annonçant la fin de Google+

. https://www.blogdumoderateur.com/google-plus-fin/

5. 83% des router ont des codes vulnérables

83% des routeurs domestiques et professionnels présentent des vulnérabilités qui pourraient être exploitées par des attaquants. Selon un rapport publié par l'American Consumer Institute sur la sécurité des routeurs, plus d'un quart de ces équipements présentent des vulnérabilités critiques à haut risque. L'étude a examiné 186 routeurs WiFi de 13 fabricants différents, dont les leaders des parts de marché, Linksys, Belkin, NETGEAR et D-Link. "Le fait de ne pas remédier aux failles de sécurité connues expose les appareils grand public à la compromission de leurs données, ce qui entraîne des activités malveillantes, le vol d'identité, la fraude et l'espionnage", selon le rapport.

https://threatpost.com/threatlist-83-of-routers-contain-vulnerable-code/137966/

6. Comment les hackers russes plombent les pc Windows

On savait que les rootkits UEFI existaient, mais personne n'en avait encore vu dans la vraie vie. C'est désormais chose faite, grâce aux limiers de l'éditeur Eset. Dans un livre blanc qu'ils viennent de publier, ils expliquent en détails les rouages techniques d'une campagne de cyberespionnage du groupe de hackers Sednit alias APT28. Ce dernier, selon plusieurs experts, serait une émanation de l'agence de renseignement militaire russe GRU. Baptisée « LoJax », cette opération – qui a visé des organisations gouvernementales en Europe centrale et Europe de l'est – s'appuie justement sur un fameux rootkit UEFI dont ils ont pu capturer et analyser un exemplaire.

https://www.01net.com/actualites/comment-les-hackers-russes-arrivent-a-plomber-les-pc-windows-pour-toujours-1536383.html

7. Un hacker contourne l'écran de verrouillage de l'iPhone

Cette fois-ci, c'est Jose Rodriguez, un hacker espagnol, qui décroche le gros lot au prix d'un effort considérable. Sa méthode de contournement, décrite dans une vidéo YouTube (en espagnol), compte pas moins de 37 étapes ! Autant dire qu'il faut avoir un peu de temps devant soi pour réaliser ce piratage. La chaîne YouTube EverythingApplePro a réalisé dans la foulée sa propre vidéo, en anglais.

https://www.01net.com/actualites/ios-12-un-hacker-contourne-l-ecran-de-verrouillage-de-l-iphone-en-37-etapes-1535615.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**.