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 de Mars 2018

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

Sommaire

Expression	Signification

I. LEXIQUE DU BULLETIN

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 Google Chrome	Une vulnérabilité a été corrigée dans Google Chrome. L'exploitation de cette vulnérabilité pourrait permettre à un attaquant distant d'accéder aux informations confidentielles. Les versions concernées sont les suivantes : Chrome OS versions antérieures à 65.0.3325.146	07/03/2018	CVE-2018-6062	64.0.3282.169 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Edge	Plusieurs vulnérabilités ont été corrigées dans Microsoft Edge. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant l'exécution de code arbitraire ou l'accès à des données confidentielles. Les systèmes affectés sont les suivants : Microsoft Internet Explorer 9, 10 et 11	15/03/2018	CVE-2018-0939	11 Télécharger	Effectuez une mise à jour du système via Windows Update	10.0
Vulnérabilité dans Mozilla Firefox et ESR	Plusieurs vulnérabilités ont été corrigées dans Firefox et Firefox ESR. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités pour prendre le contrôle d'un système affecté. Les systèmes affectés sont les suivants :	14/03/2018	CVE-2018-5143	59 Télécharger	Mettre à jour le système	10.0

	Firefox version antérieure à 59 Firefox ESR version antérieure à 52.7					
Vulnérabilité dans Internet Explorer	Plusieurs vulnérabilités ont été corrigées dans Microsoft IE. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant l'exécution de code arbitraire ou l'accès à des données confidentielles.	15/03/2018	CVE-2018-0866	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	Une vulnérabilité a été corrigée dans le CMS Joomla. L'exploitation de cette vulnérabilité permet à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. La version affectée est la suivante : CMS Joomla version antérieure à Joomla 3.8.6	15/03/2018	CVE-2018-8045	3.8.6 Télécharger	Mettre à jour le CMS	6.0

II.3 Systèmes d' exploitation

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité	De multiples vulnérabilités ont été corrigées dans le noyau Linux d'Ubun-	15/03/2018	CVE-2017-5754	4.16-rc5 Télécharger	Veuillez-vous référer au Bulletin	10.0

dans le noyau Linux d'UBUNTU	tu. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : Ubuntu 16.04 LTS, Ubuntu 17.10				de sécurité https://usn.ubuntu.com/3597-1/	
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une exécution de code à distance, une élévation de privilèges, une divulgation d'informations, un contournement de la fonctionnalité de sécurité et un déni de service	14/03/2018	CVE-2018-0900	Windows 10	Veuillez-vous référer au Bulletin de sécurité https://portal.msrc.microsoft.com/fr-FR/security-guidance/advisory/	10.0
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été corrigées dans les produits Microsoft. Elles permettent à un attaquant de provoquer une élévation de privilèges, une divulgation d'informations, une exécution de code à distance et un déni de service	13/03/2018	CVE-2018-0941	Windows 10	Veuillez-vous référer au Bulletin de sécurité https://portal.msrc.microsoft.com/fr-FR/eula	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS

Vulnérabilité dans les produits Microsoft	Microsoft a publié une mise à jour de sécurité pour corriger le problème de dysfonctionnement des périphériques USB suite à l'installation du correctif de sécurité de février 2018 (Patch Tuesday). Certains périphériques USB et périphériques intégrés cessent de fonctionner, cela se produit quand Windows ignore de manière incorrecte l'installation de la version la plus récente de certains pilotes et désinstalle les pilotes actuellement actifs pendant l'installation des mises à jour. Risque : Périphérique USB ou intégrés cessent de fonctionner. Solution : Veuillez-vous référer au bulletin de sécurité Microsoft du 07 Mars 2018: https://support.microsoft.com/en-us/help/4090913/march5-2018kb4090913osbuild16299-251					
Vulnérabilité dans SAMBA	Plusieurs vulnérabilités ont été corrigées dans Samba. Elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une élévation de privilèges.	14/03/2018	CVE-2018-1057	4.8.0 Télécharger	Effectuez une mise à jour	4.2
Vulnérabilité dans les produits Adobe	Plusieurs vulnérabilités ont été corrigées dans les produits Adobe. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une injection de code indirecte à distance (XSS).	14/03/2018	CVE-2017-4924	2018.011.20035 Télécharger	Installer les mises à jour	8.5

Vulnérabilité dans les produits CISCO	Une vulnérabilité a été corrigée dans le serveur FTP de Cisco Web Security Appliance (WSA). L'exploitation de cette vulnérabilité pourrait permettre à un attaquant distant non authentifié de se connecter au serveur FTP de l'appareil sans mot de passe valide. L'attaquant doit avoir juste un nom d'utilisateur valide.	08/03/2018	CVE-2018-0087	Contacter Cisco	Veuillez-vous référer au guide de sécurité de CISCO pour obtenir les correctifs • https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-wsa	7.8
Vulnérabilité dans PHP	Plusieurs vulnérabilités ont été corrigées dans PHP. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	02/03/2018	CVE-2018-7584	7.2.3 Téléchargez	Veuillez-vous référer au guide de sécurité de PHP pour obtenir les correctifs. http://www.php.net/ChangeLog-7.php#7.2.3	7.2

Vulnérabilité dans Juniper	Plusieurs vulnérabilités ont été corrigées dans Juniper Junos OS. Elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une élévation de privilèges.	09/03/2018	CVE-2018-0008	Contacter Juniper	Veuillez-vous référer au guide de sécurité de Juniper JSA10829 pour obtenir les correctifs. https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10830&cat=SIRT_1&actp=LIST	6.3
Vulnérabilité dans les serveurs Memcached	Deux codes d'exploit (PoC) distincts pour l'attaque DDoS de Memcached ont été publiés en ligne, ce qui pourrait causer une augmentation massive de nombre d'attaque DDoS ciblant les serveurs Memcached vulnérables exposés à internet. Il est fortement conseillé d'installer la dernière version de Memcached 1.5.6 qui désactive le protocole UDP par défaut pour empêcher ces attaques.	08/03/2018	CVE-2018-1000115	1.5.6 Télécharger	Appliquer les patchs de sécurité https://github.com/memcached/memcached/wiki/ReleaseNotes156	9.1

Vulnérabilité dans Microsoft Office	Microsoft annonce la correction de plusieurs vulnérabilités au niveau de Microsoft Office. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire à distance, l'élévation de privilèges ou l'accès à des données confidentielles.	15/03/2018	CVE-2018-0947	Contacter Microsoft	Appliquer les patchs de sécurité https://technet.microsoft.com/fr-fr/security/bulletins	7.1

III. ACTUALITÉS

1. Pourquoi la faille Spectre nous hantera toujours….

Trois mois après la révélation retentissante des failles Meltdown et Spectre, on semble enfin entrevoir la fin du tunnel. Il y a quelques jours, Microsoft annonçait ainsi la diffusion des patchs matériels pour Spectre directement depuis le catalogue de Microsoft Update, quel que soit le modèle de PC, pour peu qu'il soit équipé d'un processeur Intel. Un grand soulagement. Les utilisateurs ne se perdront plus dans le labyrinthe des pages support des constructeurs, ce qui était une grande source de confusion.

http://www.01net.com/actualites/pourquoi-la-faille-spectre-continuera-longtemps-de-hanter-nos-processeurs-1392225.html

2. Une extension chrome qui vous identifie par la façon dont vous tapez au clavier

Chaque personne a une façon différente de taper au clavier. C'est le constat qui a servi de point de départ à la société TypingDNA pour concevoir une extension pour le navigateur Chrome destinée à identifier un utilisateur. Elle ne remplace pas totalement le traditionnel mot de passe mais agit dans le cadre d'une authentification à deux facteurs, c'est-à-dire qui s'effectue en deux étapes.

http://www.01net.com/actualites/cette-extension-chrome-vous-identifie-par-la-facon-dont-vous-tapez-au-clavier-1396253.html

3. Le VPN Onavo de facebook collecte en douce les données des utilisateurs

Rachetée en 2013 par Facebook, l'appli mobile VPN « Onavo Protect » n'inspirait déjà pas une grande confiance, surtout si on lit les conditions d'utilisation. Celles-ci montrent que ce service sert surtout à analyser le comportement des utilisateurs à des fins de marketing, en s'appuyant sur le trafic réseau qui passe par les serveurs d'Onavo. Le chercheur en sécurité Will Strafach vient de rajouter une couche d'inconfort en analysant la version du logiciel sous iOS. Il s'avère que celle-ci envoie tout un tas de données directement à la maison mère Facebook.

http://www.01net.com/actualites/onavo-protect-le-vpn-de-facebook-collecte-en-douce-les-donnees-des-utilisateurs-1391192.html

4. Les cookies vont t'ils disparaitre ?

C'est une véritable levée de boucliers à laquelle doivent faire face les députés européens. Celle de grands médias européens unis dans une lettre ouverte pour lutter contre l'application du nouveau règlement sur les données personnelles e-Privacy. Ils sont furieux que le texte prévoit de confier la gestion des cookies à des logiciels de type navigateurs et que l'internaute puisse les refuser une fois pour toute et non au cas par cas. Difficile, selon eux, de continuer à analyser finement leur audience ou de la monétiser au mieux.

http://www.01net.com/actualites/les-cookies-qui-disent-tout-de-notre-vie-en-ligne-vont-ils-vraiment-disparaitre-1391555.html

5. Cortana permettrait de pirater des pc verrouillés

Les utilisateurs avisés le savent bien : quand on doit s'absenter de son PC, il faut toujours verrouiller son poste. Cette procédure évite qu'une tierce personne, qui passerait par-là, ne puisse accéder à l'ordinateur ni vu ni connu. Ça, c'est la théorie. En pratique, il s'avère que jusqu'à une période récente, on pouvait contourner ce verrouillage grâce à une fonctionnalité intégrée dans Windows 10, à savoir l'assistant Cortana.

http://www.01net.com/actualites/windows-10-cortana-permettait-de-pirater-les-pc-verrouilles-1390557.html

6. Kali le linux des hackers disponible sur Windows store mais bloqué pas defender

Depuis que Windows 10 a intégré un sous-système Linux, les utilisateurs peuvent installer des machines virtuelles Linux directement depuis Windows. Jusqu'à présent, la boutique de Microsoft proposait trois distributions : Ubuntu, Suse et OpenSuse.

http://www.01net.com/actualites/kali-le-linux-des-hackers-disponible-sur-windows-store-mais-bloque-par-defender-1389140.html

7. Une carte SIM pour chiffrer ses communications

Jusqu'à présent, pour sécuriser ses communications mobiles, il n'y avait pas trop le choix : des applications de type Telegram pour le grand public et des smartphones pas forcément sexy et très limités au niveau applicatif pour les services gouvernementaux et les entreprises. Ces derniers disposent désormais d'une nouvelle alternative. Il s'agit d'une carte SIM certifié EAL 4+ permettant de chiffrer de bout en bout voix, SMS et data : la Cyber SIM d'Orange, présentée la semaine dernière au salon du Mobile World Congress

http://www.01net.com/actualites/une-carte-sim-pour-chiffrer-ses-communications-1386816.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**.