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'Août 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 Google Chrome	De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions concernées sont celles antérieures à 68.0.3440.106 pour Windows, Mac et Linux	10/08/2018	–	68.0.3440.106 Télécharger	Mettre à jour le navigateur	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome OS	Google annonce des vulnérabilités non spécifiées sur Chrome OS versions antérieures à 68.0.3440.87 (Platform version: 10718.71.2/3)	08/08/2018	–	68.0.3440.106 Télécharger	Effectuez une mise à jour du système	9.0
Vulnérabilité dans le Noyau Linux de SUSE	Une vulnérabilité a été découverte dans le noyau Linux de SUSE. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : SUSE Linux Enterprise Live Patching 12-SP3	10/08/2018	CVE-2018- 3665	4.18.1 Télécharger	Effectuez une mise à jour du système	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	L'équipe de sécurité de Drupal annonce la correction d'une vulnérabilité dans certaines versions du CMS Drupal. L'exploitation de cette vulnérabilité peut permettre à un attaquant le contournement de la politique de sécurité. Les versions concernées sont les suivantes : 8.x antérieures à 8.5.6	10/08/2018	–	8.6.0 Télécharger	Mettre à jour le CMS	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Mozilla Thunderbird	Plusieurs vulnérabilités ont été corrigées dans Mozilla Thunderbird. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités pour prendre le contrôle d'un système affecté. Les versions affectées sont les suivantes : Mozilla Thunderbird 60	07/08/2018	CVE-2018-12367	60.0.2 Télécharger	Mettre à jour le système	8.4
Vulnérabilité dans Samba	De multiples vulnérabilités ont été découvertes dans Samba. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.	14/08/2018	CVE-2018-10919	4.8.4 Télécharger	Veuillez-vous référer au bulletin de sécurité Samba https://www.samba.org/samba/security/CVE-2018-10919.html	10.0

Vulnérabilité dans certaines imprimantes HP	Deux vulnérabilités de sécurité ont été corrigées dans certaines imprimantes HP. Un fichier malveillant, spécialement conçu, pourrait provoquer un débordement de la mémoire, ce qui peut permettre l'exécution de code à distance.	06/08/2018	CVE-2018-5925	Contacter HP	Effectuez une mise à jour du 03/07/18 https://support.hp.com/us-en/document/c06097712	4.2
Vulnérabilité dans les produits VMware	Plusieurs vulnérabilités ont été corrigées dans certain produits VMware. Un attaquant pourrait exploiter ces vulnérabilités pour obtenir des informations confidentielles.	07/06/2018	CVE-2018-3646	Contacter VMware	Veuillez-vous référer au bulletin de sécurité de VMware https://www.vmware.com/security/advisories/VMSA-2018-0020.html	8.0

Vulnérabilité dans le produit VMware Horizon	Une vulnérabilité a été corrigée dans VMware Horizon. Un attaquant pourrait exploiter cette vulnérabilité pour obtenir des informations confidentielles. Les versions vulnérables sont : VMware Horizon Client versions antérieures à 4.8.1 sur Linux, et VMware Horizon 7 version antérieure à 7.5.1	08/08/2018	CVE-2018-6970	VMware Horizon 7.5.1 Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2018-0019.html	6.2
Vulnérabilité dans les microprocesseurs Intel	Intel a publié des recommandations pour remédier à une vulnérabilité appelée ‘’L1 Terminal Fault (L1TF)’’ qui affecte plusieurs microprocesseurs Intel. Un attaquant pourrait exploiter cette vulnérabilité pour obtenir des informations sensibles. Intel® Core™ i7 processor (45nm et 32nm)	15/08/2018	CVE-2018-3646	Contacter Intel	Veuillez-vous référer au bulletin de sécurité https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html	10.0

Vulnérabilité dans les produits Cisco prime Collaboration Provisioning	Cisco annonce la correction d'une vulnérabilité au niveau de la fonctionnalité de changement de mot de passe de son produit « Cisco Prime Collaboration Provisioning ». L'exploitation de cette vulnérabilité peut permettre à un attaquant distant authentifié de causer un déni de service. Les systèmes affectés sont les suivants : Cisco Prime Collaboration Provisioning versions antérieures à 12.3	02/08/2018	CVE-2018-0391	12.3 Contacter Cisco	Veuillez-vous référer au bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180801-pcp-dos	4.0

III. Actualités

1. Pirater les élections américaines? Littéralement un jeu d'enfant

À l'heure où les manipulations entourant l'élection de Donald Trump demeurent inquiétantes, une révélation plus étonnante encore vient d'être dévoilée par un enfant de 11 ans. Les sites Internet mis à disposition par certains États pour le vote électronique sont de véritables passoires.

https://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-844913-pirater-elections-americaines-litteralement-jeu-enfant.html

2. Google récupère votre position, même si vous refusez d'être suivi

C'est l'agence de presse Associated Press qui a révélé dans un long article les pratiques mises en place par Google pour suivre vos déplacements et vos différents itinéraires, même lorsque l'utilisateur a désactivé l'historique des positions dans Google Maps ou d'autres applications développées par le moteur de recherche.

https://www.clubic.com/internet/univers-google/google-maps/actualite-844916-google-recupere-localisation-refusez-suivi.html

3. Whatsapp, la messagerie victime d'une sévère attaque

Ce sont les spécialistes de la cybersécurité israélienne Dikla Barda, Roman Zaikin et Oded Vanunu, de Check Point Research (CPR), qui ont décelé une énorme faille révélée mercredi et qui pourrait avoir de multiples conséquences à différentes échelles. Au début de l'année, WhatsApp recensait un total de 65 milliards de messages échangés chaque jour, et un peu plus d'un milliard de groupes. L'équipe de CPR a identifié trois méthodes d'attaque possibles, qui font état d'une réelle vulnérabilité de l'application de plus en plus populaire rachetée par Facebook en février 2014.

https://www.clubic.com/application-mobile/whatsapp/actualite-844866-whatsapp-messagerie-victime-severe-faille.html

4. Malwarebytes débarque sur iOS

Bien connue des utilisateurs de Windows notamment, l'application Malwarebytes va désormais débarquer sur iOS afin de permettre aux utilisateurs d'iPhone de débarrasser leur mobile d'un grand nombre d'éléments indésirables, en plus de leur fournir de nouvelles protections.

https://www.clubic.com/antivirus-securite-informatique/actualite-844827-malwarebytes-ios.html

5. La nouvelle trouvaille des hackers chinois

Oui, en 2018, le CD vérolé reste pour les pirates chinois une arme crédible : selon le Centre pour la Sécurité sur Internet (The Multi-State Information Sharing and Analysis Center, MS-ISAC), une organisation américaine regroupant gouvernement et grandes entreprises, plusieurs institutions américaines ont reçu des lettres envoyées par la poste avec un magnifique mini CD gravé en bonus.

https://www.01net.com/actualites/la-nouvelle-trouvaille-des-hackers-chinois-les-cd-graves-envoyes-par-la-poste-1497931.html

6. Le Gouvernement américain interdit à ses employés d'utiliser des appareils Huawei-ZTE

Cette interdiction est la conséquence de plusieurs années de débats et de controverses touchant à la sécurité nationale américaine. Dans l'histoire, ZTE ne s'en sort pas si mal, le Sénat US ayant voté une mesure interdisant purement et simplement l'entreprise de travailler avec des constructeurs américains, ce qui lui aurait barré la route de composants indispensables pour ses produits (les smartphones de ZTE utilisent des processeurs de Qualcomm, par exemple).

https://www.journaldugeek.com/2018/08/15/gouvernement-americain-interdit-a-employes-dutiliser-appareils-huawei-zte/

7. La Russie dans le top 10 de l'UIT

Le classement est dominé par le Singapour, suivi par les États-Unis et la Malaisie. Viennent ensuite l'Oman, l'Estonie, la République de Maurice et l'Australie, tandis que la France arrive en 8e position avec la Géorgie, et le Canada est quant à lui classé 9e. La Russie a été classée 10e pays du monde en termes de cybersécurité par l'Union internationale des télécommunications (UIT), a annoncé le ministère russe des Communications.

https://fr.sputniknews.com/international/201711031033727879-russie-cybersecurite-classement/

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**.