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'Avril 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	Google a publié une mise à jour de sécurité qui permet de corriger une vulnérabilité dans son navigateur Google chrome. L'exploitation de cette vulnérabilité peut permettre à un attaquant de causer un problème non spécifié par l'éditeur. Les versions affectées sont celles antérieures à 66.0.3359.139.	18/04/2018	CVE-2018-6118	66.0.3359.139 Télécharger	Mettre à jour le navigateur	7.4
Vulnérabilités dans Apple Safari	Apple annonce la correction de plusieurs vulnérabilités dans son navigateur Apple Safari. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire à distance. Les versions affectées sont les suivantes : Apple Safari, versions antérieures à la version 10.1	24.04.2018	CVE-2018-4204	Contacter Apple	Mettre à jour le navigateur	6.2

II.2 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Une vulnérabilité a été corrigée dans le CMS Drupal. Un attaquant distant pourrait exploiter cette vulnérabilité pour accéder à des informations sensibles et de réussir une attaque de type XSS. Les versions affectées sont les suivantes : Drupal 8.4.x version antérieure à 8.4.7. Drupal 8.5.x version antérieure à 8.5.2	19/04/2018	–	8.5.2 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 vulnérabilité a été découverte dans Microsoft Windows. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • Windows 10 • Windows server 2016	24/04/2018	CVE-2017-5715	Windows 10	Effectuer une mise à jour via Windows Update	10.0
Vulnérabilité dans les produits Apple	Apple annonce la correction de plusieurs vulnérabilités dans son système d'exploitation mobile iOS. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire à distance ou l'élévation de privilèges. Les versions infectées sont les suivantes : Apple iOS, versions antérieures à la version 11.3.1	24/04/2018	CVE-2017- 4187	Contacter Apple	Effectuez une mise à jour du système	5.6

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits CISCO	Plusieurs vulnérabilités ont été corrigées dans les produits Cisco. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité. Les systèmes infectés sont les suivants : Cisco ASA versions 9.9.x antérieures à 9.9.2.1.	19/04/2018	CVE-2018-0241	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-wbs	5.3
Vulnérabilité dans les produits ORACLE	Oracle a publié sa mise à jour critique pour Avril 2018 afin de remédier à 254 vulnérabilités sur plusieurs produits. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités pour prendre le contrôle d'un système affecté, causer un déni de service, accéder aux informations confidentielles et exécuter du code à distance.	19/04/2018	CVE-2018-7489	Contacter ORACLE	Veuillez-vous référer au bulletin de sécurité Oracle http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html	10.0

Vulnérabilité dans les produits HP	Il a été constaté que des milliers de serveurs équipés de l'interface d'administration iLO 4 font l'objet d'attaques de type ransomware. iLO est un processeur de gestion de serveur distant embarqué sur les cartes système de serveurs Hewlett-Packard ProLiant Enterprise. Le processeur de gestion permet la surveillance et le contrôle des serveurs des sites distants. Il est à noter que les attaquants continuent d'exploiter des vulnérabilités, non corrigées par les administrateurs malgré l'existence de patch, pour gagner l'accès aux serveurs via ces interfaces et ainsi crypter les disques durs. Les systèmes infectés sont les suivants : Serveurs HPE administrables via les interfaces iLO 4. Solutions : Il est recommandé que la gestion et l'administration des interfaces iLO 4 ou toute autre interface de commande à distance similaire soient correctement sécurisées en respectant certaines mesures par exemple: • Restreindre l'accès à ces interfaces en mettant une politique de filtrage appropriée. • Pour les accès distants le trafic doit emprunter un tunnel VPN. - -					
Vulnérabilité dans les produits Siemens	Siemens annonce la correction d'une vulnérabilité affectant certains de ses produits industriels. Un attaquant peut exploiter cette vulnérabilité pour causer un déni de service à distance.	14/04/2018	CVE-2018-4832	Contacter SIEMENS	Effectuez une mise à jour du système	10.0

Vulnérabilité dans Symantec Norton Core	Une vulnérabilité a été corrigée dans Symantec Norton Core. L'exploitation de cette vulnérabilité peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes infectés sont les suivants : Norton Core versions antérieures à v237	02/05/2018	CVE-2018-5234	V237 Télécharger	Effectuez une mise à jour à partir de ce lien https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20180430_00	10.0
Vulnérabilité dans PHP	De multiples vulnérabilités ont été corrigées dans PHP. L'exploitation de ces vulnérabilités peut permettre à un attaquant de causer des problèmes de sécurité non spécifiés par l'éditeur. Les systèmes infectés sont les suivants : PHP versions 7.2.x antérieures à 7.2.5 PHP versions 7.1.x antérieures à 7.1.17	26/04/2018	–	7.2.5 Télécharger	Effectuer une mise à jour du système	7.3
Vulnérabilité dans Windows Host Compute Service Shim Library	Une vulnérabilité a été corrigée dans Windows Host Compute Service Shim library (hcsshim). Un attaquant distant pourrait exploiter cette vulnérabilité pour prendre le contrôle d'un système affecté.	02/05/2018	CVE-2018-8115	–	Correctif disponible via Windows Upadte	9.1

III. ACTUALITÉS

1. Twitter appelle 330 millions d'utilisateurs à changer leur mot de passe

C'est un petit bug qui pourrait causer de nombreux soucis : Twitter appelle ses 330 millions d'utilisateurs à changer leur mot de passe. La raison de cette alerte est un bug dans la gestion du stockage des mots de passe, comme l'explique le responsable technique de l'entreprise, Parag Agrawal. En théorie, les mots de passe sont stockés de manière chiffrée sur les serveurs, mais un bug a causé « un stockage de ces mots de passe en clair sur un fichier de log interne ». Selon Mr Agrawal, « Le bug est réglé et notre enquête ne montre aucune tentative d'intrusion ou une mauvaise utilisation (du fichier de log, ndr) par quiconque ».
http://www.01net.com/actualites/twitter-appelle-330-millions-d-utilisateurs-a-changer-leur-mot-de-passe-1437117.html

2. Rencontres sur Facebook, «se liker» et plus si affinités

A peine un mois après la révélation d'un détournement massif de données de près de 90 millions d'utilisateurs de Facebook, le PDG du premier réseau social aux deux milliards d'usagers vient de créer la surprise en annonçant son arrivée sur le marché de la rencontre amoureuse. Un univers hyperconcurrentiel dont l'activité consiste précisément à rapprocher les données les plus intimes de ses adeptes pour «matcher» leurs profils avant plus si affinités.

http://www.liberation.fr/france/2018/05/02/rencontres-sur-facebook-se-liker-et-plus-si-affinites_1647367

3. Un fichier sur une clé USB pour faire planter Windows

Bonne nouvelle pour les petits farceurs. Le chercheur en sécurité Marius Tivadar de Bitdefender vient de publier sur GitHub une méthode pour faire planter Windows à l'aide d'un simple fichier. L'expert, en effet, a trouvé une faille dans la manière dont Windows gère les images système NTFS. Il avait trouvé ce bug en juillet 2017 et a immédiatement alerté Microsoft, mais ce dernier n'a pas jugé bon d'apporter un correctif. Pour susciter la panne, il faudrait en effet « un accès physique ou une attaque par ingénierie sociale », écrit la firme de Redmond dans un email. Bref, ce ne serait pas suffisamment dangereux pour développer un patch.

http://www.01net.com/actualites/un-fichier-sur-une-cle-usb-suffit-pour-faire-planter-windows-1432049.html

4. Des Hackers trouvent le moyen d'ouvrir des millions de chambres d'hôtel

Si vous passez quelques nuits à l'hôtel, attention à ne pas y laisser des affaires de valeur. Les serrures électroniques d'un grand nombre de chambres sont en effet vulnérables. Il suffit qu'un pirate dispose de l'une des cartes d'accès de l'hôtel, même ancienne, pour créer en quelques minutes une clé-maître qui permet d'accéder à toutes les chambres.

http://www.01net.com/actualites/des-hackers-ont-trouve-le-moyen-d-ouvrir-des-millions-de-chambres-d-hotel-1431350.html

5. Webstresser le plus gros service DDos a été démantelé

Clap de fin pour WebStresser, un service en ligne payant qui permettait de lancer des attaques par déni de service distribué (DDoS). Europol a annoncé hier son démantèlement dans le cadre de l'opération de police « Power Off ». Celle-ci a été menée en collaboration, entre autres, avec les polices néerlandaise et britannique. Les administrateurs ont été arrêtés. Ils résidaient aux Royaume-Uni, en Croatie, au Canada et en Serbie. Leurs serveurs ont été également été saisis. Ils étaient hébergés aux Pays-Bas, en Allemagne et aux Etats-Unis.

http://www.01net.com/actualites/webstresser-le-plus-gros-service-de-ddos-a-la-demande-a-ete-demantele-1430212.html

6. Double authentification pourquoi et comment ?

Si vous passez la moitié de votre vie sur Internet, certains vous l'auront peut-être déjà dit, mais il faut A-B-S-O-L-U-M-E-N-T passer à la double authentification, cette technique qui consiste à valider un mot de passe par exemple par l'envoi d'un code par SMS ou par une clé de sécurité. Pourquoi ? Parce que de nos jours, un mot de passe n'est plus suffisant pour sécuriser l'accès à un service en ligne.

http://www.01net.com/actualites/double-authentification-pourquoi-il-faut-s-y-mettre-et-comment-1423251.html

7. Microsoft propose une extension anti-phishing pour le navigateur chrome

Microsoft vient de corriger plusieurs failles critiques dans la gestion des polices de caractères de Windows. Une simple police piégée placée sur un site web ou dans un document suffisait à prendre le contrôle d'un PC. Simple et terriblement efficace.

http://www.01net.com/actualites/microsoft-propose-une-extension-anti-phishing-pour-le-navigateur-chrome-1422931.html

8. Ccleaner : comment des pirates ont réussi à infecter 2millions d'utilisateurs

L'affaire avait fait grand bruit. En septembre 2017, l'éditeur de CCleaner, Piriform, annonçait que certaines versions de son célèbre logiciel utilitaire étaient vérolées. Des pirates avaient réussi à introduire dans l'exécutable une backdoor avant même sa diffusion par les serveurs de mise à jour. Au total, 2,27 millions d'utilisateurs ont été infectés par ce malware dont le but était d'analyser le contexte de l'ordinateur et, le cas échéant, d'installer un « downloader », c'est-à-dire un malware dont le but est d'installer d'autres malwares. Le downloader n'a finalement été installé que sur une quarantaine de machines, au sein d'entreprises high-tech. Preuve qu'il s'agissait d'une opération très ciblée

http://www.01net.com/actualites/ccleaner-comment-des-pirates-ont-reussi-a-infecter-2-millions-d-utilisateurs-1422411.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**.