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 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

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	Plusieurs vulnérabilités ont été corrigées dans Google Chrome Os. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer un comportement non spécifié par l'éditeur. Les versions concernées sont les suivantes : Google Chrome OS versions antérieures à 65.0.3325.184 (Platform version : 10323.62.0/1)	26/03/2018	CVE-2018-6062	64.0.3325.184 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Mozilla Firefox	Une vulnérabilité a été corrigée dans Mozilla Firefox. L'exploitation de cette vulnérabilité peut permettre à un attaquant de provoquer une exécution de code arbitraire et un déni de service.	27/03/2018	CVE-2018-5148	59.0.2 Télécharger	Mettre à jour le système	10.0

II.2 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	L'équipe de sécurité Drupal annonce la correction d'une critique vulnérabilité ciblant Drupal 7.x et 8.x. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant d'exécuter du code arbitraire à distance et de prendre le contrôle complet du site compromis. Les versions affectées sont les suivantes : Drupal 7.x, 8.3.x, 8.4.x, et 8.5.x	29/03/2018	CVE-2018-8045	8.5.1 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 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 un déni de service, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : SUSE OpenStack Cloud 6, SUSE Linux Enterprise Debuginfo 11-SP4	30/03/2018	CVE-2018-5333	3.12.43-52.6.1 Télécharger	Se référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20180848-1/	10.0
Vulnérabilité dans les produits Cisco IOS XE	Plusieurs vulnérabilités ont été corrigées dans Cisco IOS XE. Elles permettent à un attaquant distant non authentifié de se connecter à un périphérique exécutant une version affectée du logiciel Cisco IOS XE avec le nom d'utilisateur et le mot de passe par défaut utilisés lors du démarrage initial, d'exécuter du code arbitraire à distance et de causer un déni de service. Les systèmes affectés sont les suivants : Cisco IOS XE versions 16.X.	29/03/2018	CVE-2018-0171	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-20180328-xesc	7.8

Vulnérabilité dans Microsoft Windows	Le correctif de Microsoft concernant la critique vulnérabilité ‘’Meltdown’’ ne parvient pas à protéger la mémoire du noyau lorsqu’il est installé sur un système Windows 7 x64 ou Windows Server 2008 R2 x64, un processus non privilégié s’avère capable de lire et d'écrire l'intégralité de l'espace mémoire disponible pour le noyau Windows. Microsoft a publié des mises à jour de sécurité pour corriger cette vulnérabilité dans les systèmes concernés. L'exploitation de cette vulnérabilité peut permettre à un attaquant de prendre le contrôle d'un système affecté et d’accéder aux informations confidentielles.	30/03/2018	CVE-2018-1038	Windows 10	Se référer au Bulletin de sécurité https://portal.msrc.microsoft.com/en-US/security-guidance	10.0
Vulnérabilité dans MikroTiK RouterOS	Une vulnérabilité a été corrigée dans MikroTiK RouterOS. L'exploitation de cette vulnérabilité pourrait permettre à un attaquant distant de provoquer une exécution de code arbitraire à distance et de prendre le contrôle du système affecté.	28/03/2018	CVE-2018-7445	Contacter Mikrotik	Appliquer les patchs de sécurité https://mikrotik.com/download	7.1

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Malwarebytes	Une vulnérabilité a été corrigée dans l'implémentation des mécanismes de chiffrement et d'autorisation au niveau du logiciel de protection contre les Malwares Malwarebytes. L'exploitation de cette vulnérabilité peut permettre à un attaquant de prendre le contrôle de la fonctionnalité de liste blanche pour permettre l'exécution des applications non autorisées, y compris des logiciels malveillants et des sites Web malveillants.	22/03/2018	CVE-2016-10717	3.4.4 Télécharger	Mettre à jour le système	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 Tenable Nessus	Une vulnérabilité a été corrigée dans Tenable Nessus. L'exploitation de cette vulnérabilité peut permettre à un attaquant une élévation de privilèges.	22/03/2018	CVE-2018-1141	7	Effectuez une mise à jour	6.2

Vulnérabilité dans Mozilla Thunderbird	Plusieurs vulnérabilités ont été corrigées dans Mozilla Thunderbird. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une élévation de privilèges. Les systèmes affectés sont les suivants : Mozilla Thunderbird versions antérieures à 52.7	26/03/2018	CVE-2018-5146	52.7 Télécharger	Effectuez une mise à jour du système	10.0
Vulnérabilité dans PHP	De multiples vulnérabilités ont été découvertes dans PHP. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un déni de service et un contournement de la politique de sécurité.	02/03/2018	CVE-2018-7584	7.2.4 Téléchargez	Veuillez-vous référer au guide de sécurité de PHP pour obtenir les correctifs. http://php.net/ChangeLog-5.php#5.6.35	7.2
Vulnérabilité dans les produits Apple	De multiples vulnérabilités ont été découvertes dans les produits Apple. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une exécution de code arbitraire et un déni de service à distance.	30/03/2018	CVE-2018-4174	Contacter Apple	Veuillez-vous référer au guide de sécurité d' Apple pour obtenir les correctifs. https://support.apple.com/en-us/HT208697	6.3

Vulnérabilité dans Apache Struts 2	Une vulnérabilité a été corrigée dans Apache Struts 2. Elle permet à un attaquant de provoquer un déni de service à distance lors de l'utilisation d'une requête malveillante avec des données XML spécialement conçues	30/03/2018	CVE-2018-1327	2.5.16 Télécharger	Appliquer les patchs de sécurité https://cwiki.apache.org/confluence/display/WW/S2-056	9.1

III. ACTUALITÉS

1. Coinhive le bout de code qui colonise le web

Connaissez-vous Coinhive ? Vous devriez, car ce petit code Javascript qui ne fait qu'une dizaine de lignes est devenu en très peu de temps l'une des principales menaces sur le radar des éditeurs antivirus. Totalement inconnu il y a encore six mois, le service Coinhive permet de miner des moneros, une cryptomonnaie alternative au bitcoin, directement dans un navigateur. Il suffit de l'intégrer dans une page web et hop, dès qu'un internaute s'y connecte, le code puise dans les ressources de sa machine pour exécuter le fameux calcul de preuve cryptographique au sein d'un pool de minage qui regroupe tous les autres utilisateurs du script.

http://www.01net.com/actualites/coinhive-un-petit-bout-de-code-qui-colonise-le-web-et-attire-les-pirates-1407943.html

2. Windows 7 le patch anti Meltdown crée une faille encore plus grande

Parfois on croit bien faire, mais en fait... c'est pire. En janvier dernier, Microsoft a publié ses patchs contre Meltdown, cette fameuse faille dans les processeurs Intel qui permet d'accéder à la zone mémoire du kernel. Il s'avère maintenant que ce patch a rendu la situation encore plus dangereuse sur les ordinateurs Windows 7 et Windows Server 8 R2 en mode 64 bits. *« Il a permis à n'importe quel processus de lire le contenu total de la mémoire avec un débit de l'ordre du gigabit/s. Oh, il était également possible de modifier des zones arbitraires de mémoire »*, explique Ulf Frisk, qui a découvert ce bug. En d'autres termes, n'importe quel petit malware pouvait, au travers de cette vulnérabilité, voler les secrets les plus confidentiels qui se trouvaient dans la RAM.

http://www.01net.com/actualites/windows-7-le-patch-anti-meltdown-a-cree-une-faille-encore-plus-grande-1406582.html

3. IOS une faille qui permet de diffuser des QR codes malveillants

Si vous avez un iPhone et que vous avez l'habitude de scanner des QR codes avec l'application Caméra, prenez garde ! Une faille permet aux pirates de tromper aisément l'utilisateur et de le rediriger vers un site piégé alors qu'il croît se rendre vers un site de confiance. Découverte par le chercheur en sécurité Roman Mueller, cette vulnérabilité est liée au parseur d'URL qui, visiblement, a du mal à gérer certaines chaînes de caractères.

http://www.01net.com/actualites/ios-une-faille-permet-de-diffuser-des-qr-codes-malveillants-1406485.html

4. Cambridge Analytica un scandale qui pourrait coûter cher à Facebook

Depuis que Christopher Wylie a révélé que la société Cambridge Analytica a exploité les données de 50 millions d'utilisateurs Facebook, le réseau social redoute la fuite de ses abonnés et la baisse de ses revenus publicitaires. Mais il va devoir aussi faire face à une sérieuse enquête de la FTC (Federal Trade Commission), le régulateur du commerce américain. Qui vient de publier un communiqué de presse où il annonce s'intéresser non seulement à Cambridge Analytica mais aussi à Facebook.

http://www.01net.com/actualites/cambridge-analytica-un-scandale-qui-pourrait-couter-tres-cher-a-facebook-1405495.html

5. La NSA surveille de très près les transactions Bitcoin

L'archive d'Edward Snowden n'est visiblement pas encore épuisée. Le site The Intercept vient de révéler une série de documents qui datent de 2012 et 2013 et qui montrent que la NSA est également très intéressée par les utilisateurs de bitcoin. Déjà à l'époque, l'agence ne se limitait pas à examiner la blockchain, le registre des transactions bitcoin, mais procédait à la récolte de données sensibles permettant d'identifier les émetteurs et les récepteurs : adresses MAC, adresses IP, activité web, mots de passe, etc.

. http://www.01net.com/actualites/la-nsa-surveille-de-tres-pres-les-transactions-bitcoin-1401180.html

6. Firefox : une faille de plus de 9 ans dans le gestionnaire des mots de passe

Si vous stockez vos mots de passe dans Firefox et que vous les chiffrez au moyen d'un mot de passe maître (MPM), sachez que le niveau de sécurité est moins élevé qu'avec un gestionnaire en bonne et due forme comme KeePass ou Lastpass. Le développeur Wladimir Palant, qui a notamment créé AdBlock Plus, a récemment jeté un œil dans le code source du navigateur. Il a découvert que ce MPM n'est que faiblement protégé. Pourquoi ? Car il n'est haché que de manière simple, à l'aide de l'algorithme SHA1 et d'un sel cryptographique.

http://www.01net.com/actualites/firefox-une-faille-traine-dans-le-gestionnaire-de-mots-de-passe-depuis-9-ans-1400333.html

7. Appels et sms enregistrés sur Facebook

D'après son créateur, Facebook n'est pas un média. Mais Facebook s'essaie parfois au « fact checking », comme l'indique le titre d'un billet posté hier 25 mars par l'entreprise. Le message fait suite aux articles évoquant l'enregistrement de l'historique des appels et SMS des utilisateurs par le géant américain. En téléchargeant leur archive Facebook, certains d'entre eux - nous compris - avaient retrouvé la trace d'appels passés il y a plusieurs années. Seuls les smartphones sous Android sont concernés.

http://www.01net.com/actualites/appels-et-sms-enregistres-facebook-confirme-et-s-explique-1404416.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**.