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'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 IE et Edge	Plusieurs vulnérabilités ont été corrigées au niveau des deux navigateurs de Microsoft L'exploitation de ces vulnérabilités peut permettre à un attaquant distant L'exécution de code arbitraire ou l'accès à des données confidentielles. Les versions concernées sont les suivantes : 10 et 11.	11/04/2018	CVE-2018-1020	11	Effectuer une mise à jour via Windows Update	7.3

II.2 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS WordPress	Plusieurs vulnérabilités ont été corrigées dans WordPress. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : WordPress versions antérieures à 4.9.5	04/04/2018	–	4.9.5 Télécharger	Mettre à jour le CMS	8.0

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. Elles permettent à un attaquant de provoquer une divulgation d'informations, une exécution de code à distance et un contournement des fonctionnalités de sécurité.	11/04/2018	CVE-2018-1016	Windows 10	Effectuer une mise à jour via Windows Update	10.0
Vulnérabilité dans les processeurs Intel	AMD et Microsoft ont publié des mises à jour de microcodes et de systèmes d'exploitation qui ajoutent des protections contre les attaques Spectre pour les systèmes Windows Équipés de processeurs AMD.	12/04/2018	CVE-2017-5715	Windows 10	Se référer au Bulletin de sécurité AMD et Microsoft https://support.microsoft.com/en-us/help/4093112/windows-10-update-kb4093112	5.6
Vulnérabilité dans les produits Juniper	Plusieurs vulnérabilités ont été corrigées dans les produits Juniper. Certaines d'entre elles permettent 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.	17/04/2018	CVE-2018-0023	Contacter Juniper	Solution par contournement disponible ici	5.5

Vulnérabilité dans Google Chrome OS	Plusieurs vulnérabilités ont été corrigées dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions concernées sont les suivantes : Google Chrome OS versions antérieures à 65.0.3325.209 (Platform version : 10323.67/68)	11/04/2018	-	64.0.3325.209 Télécharger	Mettre à jour le système	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits F5 BIG-IP	Plusieurs vulnérabilités ont été corrigées dans certains produits F5 BIG-IP. L'exploitation de ces vulnérabilités peut permettre à un attaquant de causer un déni de service à distance et un contournement de la politique de sécurité.	14/04/2018	CVE-2018-5506	Contacter F5 BIG-IP	Effectuez une mise à jour	5.3

Vulnérabilité dans Microsoft Wireless Keyboard 850	Une vulnérabilité de contournement de fonctionnalité de sécurité existe dans le Microsoft Wireless Keyboard 850. Elle permettrait à un attaquant de réutiliser une clé de cryptage AES pour envoyer des frappes à d'autres claviers ou lire des frappes envoyées par d'autres claviers. Alias Microsoft Wireless Keyboard 850 Security Feature Bypass Vulnerability.	11/04/2018	CVE-2018-8117	Windows 10	-	-
Vulnérabilité dans les VMware vCenter Server Appliance	VMware vCenter Server Appliance (vCSA) (6.5 avant 6.5 U1d) contient une vulnérabilité d'escalade de privilèges locale via le plugin 'showlog'. Une exploitation réussie de ce problème permettrait à un utilisateur à privilèges limités d'obtenir des privilèges équivalents à ceux de l'utilisateur root du système.	11/04/2018	CVE-2017-4943	6.5 U1d	Mettre à jour en version 6.5 U1d	7.8
Vulnérabilité dans VMware vRealize Automation	Plusieurs vulnérabilités ont été corrigées dans VMware vRealize Automation. L'exploitation de cette vulnérabilité peut entraîner le vol d'une session d'utilisateur vRA valide. Les systèmes affectés sont les suivants : vRealize Automation versions antérieures à 7.4.	14/04/2018	CVE-2018-6959	7.4 Télécharger	Effectuez une mise à jour du système	10.0

Vulnérabilité dans Citrix XenServer	Plusieurs vulnérabilités ont été corrigées dans Citrix XenServer. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : Citrix XenServer 6.5SP1, Citrix XenServer 6.2SP1, Citrix XenServer 6.0.2 Common Criteria	09/04/2018	CVE-2018-7541	7.4 Télécharger	Un patch est disponible à l'adresse https://support.citrix.com/article/CTX232096	7.2
Vulnérabilité dans Windows Defender	Une vulnérabilité a été corrigée dans Windows Defender. Cette vulnérabilité est due à une analyse incorrecte d'un fichier spécialement conçu par "Microsoft Malware Protection" ce qui entraîne une altération de la mémoire. Un attaquant qui parviendrait à exploiter cette vulnérabilité pourrait exécuter du code arbitraire dans le contexte de sécurité du compte LocalSystem et prendre le contrôle du système. L'attaquant pourrait alors installer des programmes, afficher, modifier ou supprimer des données, ou créer des comptes dotés de tous les privilèges.	04/04/2018	CVE-2018-0986	-	Correctif disponible via Windows Upadte	7.3
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.	11/04/2018	CVE-2018-1014	MS Office 2016	Correctif disponible via Windows Upadte	9.1

III. ACTUALITÉS

1. Comment les Etats Unis d'Amérique détecte les cyberattaques ?

Les cyberattaques se multiplient et deviennent de plus en plus sophistiquées. L'alerte récente en provenance des Etats-Unis et du Royaume-Uni, à propos d'une campagne mondiale d'attaques sur les équipements réseaux menées par les Russes selon eux, montre que l'espace cyber est devenu un enjeu de sécurité nationale de premier plan.

http://www.01net.com/actualites/comment-l-etat-detecte-t-il-les-cyberattaques-1421510.html

2. Microsoft annonce un nouvel OS basé sur Linux

Le géant du logiciel vient de dévoiler un nouveau système d'exploitation dédié aux objets connectés. Mais ce n'est pas un Windows : il aura pour coeur... un noyau Linux. Une première en 43 ans d'existence.

http://www.01net.com/actualites/microsoft-annonce-un-nouvel-os-base-sur-linux-1421297.html

3. Télégram : le nouvel eldorado des contenus illégaux

Brocardée pour avoir été utilisée par des terroristes, censurées par des états autoritaires comme la Russie, la messagerie chiffrée Telegram suscite désormais l'ire des ayants droits. Car elle est devenue une véritable plaque tournante de contenus illégaux, selon le site new-yorkais The Outline qui a mené l'enquête.

http://www.01net.com/actualites/piratage-telegram-le-nouvel-eldorado-des-contenus-illegaux-1418467.html

4. Selon les USA et le royaume unis, la Russie infecte les réseaux du monde entier

Voilà qui risque de détériorer un peu plus les relations entre trois des principales puissances économiques mondiales. Une campagne de cyberattaques de grande ampleur serait menée depuis la Russie dans le monde entier d'après les autorités américaines et britanniques.

http://www.01net.com/actualites/selon-les-etats-unis-et-le-royaume-uni-la-russie-infecte-les-reseaux-du-monde-entier-1421126.html

5. Des chercheurs exfiltrent des données sensibles d'un pc à travers sa prise de courant

Les experts de l'université Ben Gourion ont de nouveau frappé. Spécialisés dans le piratage d'ordinateurs déconnectés (« air-gapped »), ces chercheurs israéliens viennent de présenter une nouvelle manière d'exfiltrer en douce des informations sensibles. Cette fois, la fuite de données s'appuie sur le courant électrique qui alimente la machine.

http://www.01net.com/actualites/ces-chercheurs-exfiltrent-les-donnees-d-un-pc-par-sa-prise-de-courant-1420571.html

6. Windows : il était possible de pirater n'importe quel pc à l'aide des caractères piégés

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/windows-il-etait-possible-de-pirater-n-importe-quel-pc-avec-des-caracteres-pieges-1416931.html

7. Vos données font elles partie des milliards de fichiers en accès libre sur internet ?

D'après Digital Shadows, une entreprise de cybersécurité, il existe une quantité incroyable de données en accès libre sur Internet en raison de serveurs mal configurés. Après avoir scanné la Toile pendant trois mois, les experts de cette société américaine ont pu détecter plus de 1,5 milliard de documents dans des espaces de stockage ouverts à tous : des bouquets Amazon S3, des serveurs NAS, des sites Web, des accès FTP, SMB ou rsync, etc. Au total, cela fait plus 12 petaoctets. « C'est 4000 fois plus large que la fuite des Panama Papers (2,6 teraoctets) », soulignent les chercheurs de Digital Shadows.

http://www.01net.com/actualites/vos-donnees-font-elles-partie-du-15-milliard-de-fichiers-en-acces-libre-sur-internet-1413209.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**.