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 2019

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 Microsoft Edge et IE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge et IE. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.	13/03/2019	CVE-2019-0780	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans Chrome	De multiples vulnérabilités ont été découvertes dans Chrome. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et un contournement de la politique de sécurité. Les versions concernées sont les suivantes : Chrome versions antérieures à 73.0.3683.75	13/03/2019	CVE-2019-5804	73.0.3683.86 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 Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service et une exécution de code à distance.	13/03/2019	CVE-2019-0808	_	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans le noyau Linux de RedHat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de RedHat. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	14/03/2019	CVE-2018-18445	5.0.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2019:0512	10.0

Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Elles permettent à un attaquant de provoquer un déni de service et une élévation de privilèges. Les systèmes infectés sont les suivants : • Ubuntu 14.04 LTS • Ubuntu 16.04 LTS	14/03/2019	CVE-2019-6133	5.0.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3910-2/	10.0
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 une élévation de privilèges, un déni de service et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Software Development Kit 11-SP4 • SUSE Linux Enterprise Server 11-SP4 • SUSE Linux Enterprise Server 11-EXTRA • SUSE Linux Enterprise Real Time Extension 11-SP4 • SUSE Linux Enterprise High Availability Extension 11-SP4 • SUSE Linux Enterprise Debuginfo 11-SP4	14/03/2019	CVE-2019-7222	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-201913979-1/	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Joomla	De multiples vulnérabilités ont été découvertes dans Joomla! Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Joomla! versions 3.x antérieures à 3.9.4;	21/02/2019	CVE-2019-9714	3.9.4 Télécharger	Mettre à jour le CMS	10.0
Vulnérabilité dans le CMS WordPress	De multiples vulnérabilités ont été corrigées dans WordPress. Elles permettent à un attaquant de provoquer une injection de code de code indirecte à distance (XSS). Les versions affectées sont les suivantes : WordPress versions 5.1 et antérieures	13/03/2019		5.1 Télécharger	Mettre à jour le CMS	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une exécution de code à distance et un contournement de la fonctionnalité de sécurité. Les systèmes affectés sont les suivants : • Microsoft Office 2010 Service Pack 2 (éditions 64 bits) • Microsoft SharePoint Enterprise Server 2016 • Microsoft SharePoint Foundation 2013 Service Pack 1	13/03/2019	CVE-2019-0778	2019	Mettre à jour le système via Windows Update	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 atteinte à la confidentialité des données, une exécution de code à distance, une usurpation d'identité et un contournement des fonctionnalités de sécurité. Les systèmes infectés sont les suivants : • Microsoft Dynamics 365 (on-premises) version 8 • Microsoft Lync Server 2013 July 2018 Update • Nuget 4.9.4 • Skype pour Business Server 2015 March 2019 Update • Visual Studio pour Mac • Team Foundation Server 2018 Update 3.2	13/03/2019	CVE-2019-0809	–	Mettre à jour le système via Windows Update	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Microsoft .Net.	Une vulnérabilité a été corrigée dans Microsoft .Net. Elle permet à un attaquant de provoquer un contournement des fonctionnalités de sécurité. Les systèmes affectés sont les suivants : • NET Core SDK 1.1 • .NET Core SDK 2.1.500	13/03/2019	CVE-2019-0757	–	Mettre à jour le système via Windows Update	
Vulnérabilité dans les produits Adobe	De multiples vulnérabilités ont été découvertes dans les produits Adobe. Elles permettent à un attaquant de provoquer une exécution de code arbitraire. Les systèmes affectés sont les suivants : • Photoshop CC versions 19.1.7 et antérieures pour Windows et macOS • Photoshop CC versions 20.0.2 et antérieures pour Windows et macOS • Adobe Digital Editions versions 4.5.10.185749 et antérieures pour Windows	12/03/2019	CVE-2019-7094	Contacter Adobe	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/Digital-Editions/apsb19-16.html	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits VMware	De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et une élévation de privilèges. Les versions vulnérables sont : • Horizon 7 (CR) versions 7.x pour Windows antérieures à 7.8+KB67424 • Horizon 7 (ESB) versions 7.5.x pour Windows antérieures à 7.5.2+KB67401 • Horizon 6 versions 6.x pour Windows antérieures à 6.2.8+KB67401 • Workstation versions 15.x pour Windows antérieures à 15.0.3 • Workstation versions 14.x pour Windows antérieures à 14.1.6	18/03/2019	CVE-2019-5513	Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2019-0002.html	6.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits CISCO	Une vulnérabilité a été découverte dans Cisco Common Services Platform Collector. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes infectés sont les suivants : • Cisco CSPC versions 2.7.2 à 2.7.4.5 • Cisco CSPC toutes versions 2.8.x antérieures à 2.8.1.2	14/03/2019	CVE-2019-1723	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190313-cspcscv	5.3
Vulnérabilité dans les produits Intel	De multiples vulnérabilités ont été découvertes dans les produits Intel. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance.	13/03/2019	CVE-2019- 0139	Contacter Intel	Veuillez-vous référer au bulletin de sécurité https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00231.html	5.6

III. Actualités

1. WhatsApp Facebook Instagram et Messenger touchés par une énorme panne

Mise à jour, jeudi 14 mars, 17 h 30 : Après une journée de bugs et de problèmes, Facebook a indiqué, dans la fin d'après-midi du jeudi 14 mars, que la panne était terminée. Dans un Tweet, le compte officiel de Facebook explique : « Hier, dans le cadre d'un changement de configuration de nos serveurs, beaucoup de personnes ont connu des problèmes en essayant d'accéder à nos applications et à nos services. Nous avons désormais résolu ces problèmes (…). Nous sommes vraiment désolés pour ce dysfonctionnement et vous remercions pour votre patience. » Selon le site spécialise The Verge, cette panne est la plus importante à avoir affecté Facebook depuis sa création : elle a en effet, pendant vingt-quatre heures, partiellement paralysé un ensemble d'application (Facebook, Instagram, WhatsApp) utilisées, en tout, par 2,3 milliards de personnes dans le monde.

https://www.lemonde.fr/pixels/article/2019/03/13/facebook-instagram-messenger-et-whatsapp-touches-par-une-panne_5435661_4408996.html?xtor=RSS-3208

2. Les antivirus pour Android pas du tout efficaces

L'organisme de tests d'antivirus AV-Comparatives vient de publier une étude qui révèle que, sur 250 applications de sécurité Android testées, seulement 80 se sont révélées susceptibles de détecter plus de 30% des malwares, sans fausse alarme. Et seulement 23 applications se sont montrées capables de détecter tous les échantillons de malwares utilisés pour le test.

https://www.01net.com/actualites/les-antivirus-pour-android-ne-sont-pas-suffisamment-efficaces-1654543.html

3. Les pirates exploitent une faille dans chrome

Quand le chercheur en sécurité de Google Justine Schuh trouve une faille critique dans Chrome et qu'il donne publiquement le conseil de mettre à jour le navigateur « dans la minute qui suit », il vaudrait mieux obtempérer. Car, comme le dit un autre expert en sécurité sur Twitter, « il est a) en position de savoir pourquoi et b) il ne le fait pas souvent ».

https://www.01net.com/actualites/chrome-des-pirates-exploitent-de-maniere-active-une-faille-critique-1647260.html

4. Les certificats TLS se vendent sur le dark web

Quand vous vous connectez sur un site de commerce électronique, vous faites probablement attention au pictogramme qui s'affiche à côté de l'URL. S'il s'agit d'un cadenas fermé, éventuellement de couleur verte, c'est théoriquement un bon signe. Cela veut dire que le serveur Web dispose d'un certificat de sécurité en bonne et due forme, délivrée par une autorité de certification reconnue par le navigateur (ou par l'administrateur système). Parfois, le nom de l'entreprise est également affiché à côté du cadenas. Ce qui veut dire qu'il s'agit d'un certificat à validation étendue (Extended Validation, EV). Celui-ci n'est délivré par les autorités de certification qu'après des vérifications approfondies sur l'identité et la nature de l'entreprise. Sur le Web, c'est le nec plus ultra de la sécurité des connexions.

https://www.01net.com/actualites/les-certificats-tls-coeur-de-la-securite-du-web-se-vendent-desormais-sur-le-dark-web-1646684.html

5. 5G l'Allemagne poursuit son chantier malgré les menaces

L'Allemagne lance mardi les enchères pour l'octroi des chantiers de sa future 5G, sans exclure les équipementiers chinois comme Huawei, malgré les menaces de Washington de revoir la coopération sécuritaire transatlantique. "Peu importe qu'un fournisseur vienne de Suède ou de Chine, les entreprises doivent satisfaire aux exigences de certification et aux contrôles de sécurité", a jugé lundi lors d'une conférence de presse Jochen Homann, président de l'agence fédérale allemande des réseaux.

https://www.lepoint.fr/economie/huawei-5g-l-allemagne-avance-dans-son-chantier-malgre-les-menaces-americaines-19-03-2019-2302160_28.php

6. Android sans tactile ?

Aujourd'hui, l'un des objectifs de Google est de connecter un maximum de personne à la toile. Pour réaliser cet objectif, la firme a développé un programme baptisé Android Go qui propose une version allégée de son système d'exploitation et de son écosystème d'applications, pour les smartphones low-cost.

https://www.presse-citron.net/google-pourrait-il-travailler-sur-une-version-non-tactile-dandroid/

7. 2 millions de mots de passe français en ligne

Dans le petit monde des pirates informatiques, une fois qu'une donnée a été pressée comme un citron, elle est diffusée, lâchée en pâture a qui saura la récupérer. Il y a quelques heures, un pirate informatique a mis en ligne un fichier texte (.txt) comprenant 2,2 millions d'identifiants de connexion de Français. La diffusion se fait sur un site de partage de fichier anonyme. Le fichier de 70Mo n'a pas de nom. Il propose des centaines de milliers de mails et mots de passe sans indiquer d'où proviennent les données en question.

https://www.zataz.com/data-leak-2-millions-mails-mots-de-passe-francais/

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**.