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 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	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.	10/04/2019	CVE-2019-0861	-	Mettre à jour via Windows Update	8.5
Vulnérabilité dans Microsoft Internet Explorer	De multiples vulnérabilités ont été corrigées dans Microsoft Internet Explorer. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une exécution de code à distance et un contournement des fonctionnalités de sécurité. Les systèmes infectés sont les suivants : • Internet Explorer 10 • Internet Explorer 11 • Internet Explorer 9	10/04/2019	CVE-2019-0862	11.706.17134.0	Mettre à jour via Windows Update	9.0

Vulnérabilité dans Google Chrome	De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à la confidentialité des données et un problème de sécurité non spécifié par l'éditeur. Systèmes affectés : Google Chrome versions antérieures à 74.0.3729.108.	24/04/2019	CVE-2019-0861	74.0.3729.108 Télécharger	Mettre à jour le navigateur	4.6

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome OS	De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : Toutes les versions de Google Chrome OS antérieures à 73.0.3683.114 (Platform version: 11647.154.0)	23/04/2019	CVE-2019-2245	73.0.3683.114 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/04/stable-channel-update-for-chrome-os.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleChromeReleases+%28Google+Chrome+Releases%29	10.0
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 un déni de service à distance. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Server for SAP 12-SP2 • SUSE Linux Enterprise Server 12-SP2-LTSS	17/04/2019	CVE-2018-5390	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20190955-1/	10.0

Vulnérabilité dans Juniper Junos OS	De multiples vulnérabilités ont été découvertes dans Juniper Junos OS. Elles permettent à un attaquant de provoquer un déni de service et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : Juniper Junos OS versions antérieures de 15.1F6-S12 à 18.4X1	15/04/2019	CVE-2018-6924	-	Veuillez-vous référer au Bulletin de sécurité https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10937&cat=SIRT_1&actp=LIST	10.0
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et un contournement des fonctionnalités de sécurité.	01/04/2019	CVE-2019-0879	10	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. Certaines d'entre 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.	24/04/2019	CVE-2018-18347	7.6	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2019:0833	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Plusieurs vulnérabilités ont été corrigées dans Drupal. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance et de prendre le contrôle du système affecté. Les versions affectées sont les suivantes : • Drupal versions 8.6.x antérieures à 8.6.15 ; • Drupal versions 8.5.x antérieures à 8.5.15 ; • Drupal versions 7.x antérieures à 7.66;	05/04/2019	CVE-2019-10911	8.6.15 Télécharger	Mettre à jour le CMS	8.5
Vulnérabilité dans le CMS Joomla	Plusieurs vulnérabilités ont été corrigées dans le CMS Joomla. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer un contournement de la politique de sécurité et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Joomla versions antérieures 1.5.0 à 3.9.4	10/04/2019	CVE-2019-10911	3.9.5 Télécharger	Mettre à jour le CMS	6.5

II.4 SERVEUR D'APPLICATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité du serveur d'application Apache Tomcat	Apache Software Foundation annonce la disponibilité d'une mise à jour qui permet de corriger une vulnérabilité au niveau du serveur d'applications Apache Tomcat. L'exploitation de cette vulnérabilité peut permettre à un attaquant distant l'exécution de code et la prise de contrôle du système affecté. Les systèmes infectés sont les suivants • Apache Tomcat 9.0.0.M1 jusqu'à 9.0.17 • Apache Tomcat 8.5.0 jusqu'à 8.5.39 • Apache Tomcat 7.0.0 jusqu'à 7.0.93	22/03/2019	CVE-2019-0232	9.0.19 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs http://mail-archives.us.apache.org/mod_mbox/wwwannounce/201904.mbox/%3C13d878ec-5d49-c348-48d4-25a6c81b9605%40apache.org%3E	5.2

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 et une usurpation d'identité. Les systèmes infectés sont les suivants : • Team Foundation Server 2018 Update 3.2 • Team Foundation Server 2018 Update 3.2 • ChakraCore • Microsoft Exchange Server 2013 Cumulative Update 22 • Microsoft Exchange Server 2013 Cumulative Update 22	10/04/2019	CVE-2019-0871	-	Effectuez une mise à jour via Windows Update	10.0

II.5 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans produits VMware	De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer un déni de service et une élévation de privilèges. Les systèmes infectés sont les suivants : • ESXi versions 6.7 antérieures à ESXi670-201904101-SG • ESXi versions 6.5 antérieures à ESXi650-201903001 • Workstation versions 15.x antérieures à 15.0.3 • Workstation versions 14.x antérieures à 14.1.6 • Fusion versions 11.x pour OSX antérieures à 11.0.3 • Fusion versions 10.x pour OSX antérieures à 10.1.6	12/04/2019	CVE-2019-5520	Contacter VMware	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.vmware.com/security/advisories/VMSA-2019-0006.html	7.3
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	10/04/2019	CVE-2019-0831	2019	Mettre à jour le système via Windows Update	7.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Microsoft ASP.Net.	Une vulnérabilité a été corrigée dans Microsoft ASP.Net. Elle permet à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : • ASP.NET Core 2.2	11/04/2019	CVE-2019-0815	_	Mettre à jour via Windows Update	7.7
Vulnérabilité dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et une injection de code indirecte à distance (XSS). Les versions vulnérables sont : • FortiSwitch versions 6.0.0 à 6.0.1 • FortiSwitch versions 3.6.8 et antérieures • FortiAP-S versions FAP_S221E et FAP_S223E • FortiAP-W2 versions FAP_221E (Gen1/Gen2), FAP_222E et FAP_223E (Gen1/Gen2)	11/04/2019	CVE-2018-16986	Contacter Fortinet	Veuillez-vous référer au bulletin de sécurité https://fortiguard.com/psirt/FG-IR-18-356	6.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Cisco	De multiples vulnérabilités ont été découvertes dans les produits Cisco. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une élévation de privilèges. Les systèmes affectés sont les suivants : Cisco IOS XR 64-bit versions antérieures à 6.5.3 et 7.0.1 • Cisco Wireless LAN Controller versions antérieures à 8.3.150.0 • Cisco Wireless LAN Controller versions 8.4.x et 8.5.x antérieures à 8.5.140.0 • Cisco Wireless LAN Controller versions 8.6.x, 8.7.x et 8.8.x antérieures à 8.8.120.0 • Cisco Expressway Series et Cisco TelePresence Video Communication Server versions antérieures à X12.5.1	18/04/2019	CVE-2019-1800	Contacter CISCO	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190417-wlc-gui	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits IBM	De multiples vulnérabilités ont été découvertes dans les produits IBM. 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. Les systèmes affectés sont les suivants : • FortiSwitch versions 6.0.0 à 6.0.1 • FortiSwitch versions 3.6.8 et antérieures • FortiAP-S versions FAP_S221E et FAP_S223E • FortiAP-W2 versions FAP_221E (Gen1/Gen2), FAP_222E et FAP_223E (Gen1/Gen2)	27/03/2019	CVE-2019-2426	Contacter IBM	Veuillez-vous référer au bulletin de sécurité https://www-01.ibm.com/support/docview.wss?uid=ibm10876338	5.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Foxit Reader et PhantomPDF	De multiples vulnérabilités ont été découvertes dans Foxit Reader et PhantomPDF. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Foxit Reader versions antérieures à 9.5 sur Windows • Foxit PhantomPDF versions antérieures à 9.5 sur Windows	16/04/2019	CVE-2019-20316	Contacter Foxit	Veuillez-vous référer au bulletin de sécurité https://www.foxitsoftware.com/support/security-bulletins.php	2.6

III. ACTUALITÉS

1. Un gang de pirates des distributeurs automatiques aux arrêts

Le piratage de distributeurs automatique de billets (DAB) fait recette chez les cybercriminels équipés… Ces derniers agissant dans l'est de la France utilisaient la technique du jackspotting (prise de contrôle informatique du distributeur visé via démontage partiel et connexion physique sur la machine) durant la nuit afin de le vider de ses billets.

https://www.undernews.fr/hacking-hacktivisme/jackpotting-gang-pirates-dab-arrete.html

2. Black Hat SEO attention à certaines techniques de référencements

Le Black Hat SEO fait référence à des pratiques contraires à l'éthique dictée par les moteurs de recherche utilisées dans le but d'aider un site Web à atteindre un rang supérieur dans Google ou autre moteur. Les résultats peuvent être fulgurants mais peuvent aussi conduire à une forte pénalité qui fera que le site en question sera fortement déclassé dans les résultats de recherche ou bien totalement supprimé !

https://www.undernews.fr/culture-web-emploi/black-hat-seo-attention-a-ces-techniques-de-referencement.html

3. Un pirate informatique arrêté à la suite d'une panne de courant

Remonter la piste d'un pirate peut prendre beaucoup de temps … ou tenir à peu de chose. Pour le cas d'aujourd'hui, un Anonymous, c'est même fée électricité qui l'a révélé aux autorités. Janvier 2016, une cyber manifestation est lancée en ligne à l'encontre de plusieurs sites du gouvernement Français. Les Anonymous voulaient protester contre la prolongation de l'Etat d'urgence et la loi Renseignement. Plusieurs sites ministériels bloqués, dont le site du Premier Ministre, l'Assemblée Nationale ou encore la Justice. Des blocages orchestrés à coups de DDoS, Dénis Distribués de Service.

https://www.zataz.com/un-pirate-informatique-arrete-a-la-suite-dune-panne-de-courant/

4. Cybersquatting faites attention au .co si vous avez un .com

En cette période politiquement instable, il n'est plus à prouver la force des malveillances numériques. Elles peuvent prendre la forme de fake news (désinformation) diffusées sur les réseaux sociaux ; la création de faux journaux ; de cybersquatting ; d'infiltration de supports médiatiques. Sur ce dernier point, nous y reviendront dans quelques jours (ICI). Vous avez un site web, un blog en .com ? Prudence à l'usurpation d'identité, au cybersquatting, avec la possibilité d'enregistrer votre nom de domaine en .co.

https://www.zataz.com/cybersquatting-vous-avez-un-com-attention-au-danger-du-co/

5. Un hacker pirate des dizaines de milliers de GPS avec le mot de passe 123456

Un hacker qui se fait appeler L&M a réussi à pirater des dizaines de milliers de comptes utilisateurs pour deux applications GPS professionnelles. En occurrence 7.000 pour iTrack et 20.000 pour ProTrack. Ces applications mobiles, qui sont disponibles sur iOS et Android, permettent aux entreprises de gérer leurs flottes de véhicules. L'accès aux comptes des utilisateurs a permis au hacker de géolocaliser des véhicules un peu partout dans le monde.

https://www.01net.com/actualites/un-hacker-a-pirate-des-dizaines-de-milliers-de-gps-avec-le-mot-de-passe-123456-1679983.html

6. Des pirates ont détourné le DNS de plusieurs pays

Les chercheurs en sécurité de Cisco Talos viennent de publier une analyse sur un groupe de pirates baptisé « Sea Turtle ». Ces hackers, qui sont très probablement une émanation gouvernementale, ont espionné une quarantaine d'organisations dans le Moyen-Orient. Pour y arriver, ils n'ont pas hésité à pirater des registres pour pouvoir détourner plusieurs extensions nationales de noms de domaine, dont celle de l'Arménie (.AM). Ce qui leur permettait d'usurper l'identité de n'importe quel site sous cette extension. Selon Cisco Talos, c'est la première fois que l'on voit des pirates arriver à de telles extrémités dans le cadre d'opérations d'espionnage informatique.

https://www.01net.com/actualites/des-pirates-ont-detourne-le-dns-de-plusieurs-pays-1676481.html

7. Un étudiant a grillé 66 ordinateurs de sa fac avec une clé usb killer

Le 14 février dernier, un étudiant en MBA de l'université College of St Rose à New York a utilisé une clé « USB Killer » pour détruire 59 PC Windows et 7 ordinateurs Mac qui étaient installés dans les salles informatiques de l'établissement. Ce qui représente un dommage financier de 58.471 dollars.

https://www.01net.com/actualites/un-etudiant-a-grille-66-ordinateurs-de-sa-fac-avec-une-cle-usb-killer-1676008.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. Microsoft annonce la fin du support de toutes les versions de Windows 7 à partir du 14 janvier 2020. Après cette date les systèmes fonctionnant sous Microsoft Windows 7 ne recevront plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
4. 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.
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**.