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 Septembre 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 IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer un contournement de la fonctionnalité de sécurité et une exécution de code à distance. Les systèmes concernés sont les suivants : • Internet Explorer 10 • Internet Explorer 11 • Internet Explorer 9	11/09/2019	CVE-2019-1220	-	Mettre à jour le système via Windows Update	10.0
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, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	11/09/2019	CVE-2019-1300	-	Mettre à jour le système via Windows Update	9.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. La version affectée est la suivante : Android version Q sans le correctif de sécurité 2019-09-01	05/09/2019	CVE-2019-10941	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2019-09-01.html	10.0
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer un déni de service, une élévation de privilèges, une atteinte à la confidentialité des données, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	11/09/2019	CVE-2019-1294	10	Mettre à jour le système via Windows Update	10.0

II.1 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Wordpress	Le plugin wp-d3 de version antérieure à 2.4.1 pour wordpress présente une vulnérabilité de type Cross-site request forgery (CRSF)	13/09/2019	CVE-2016-10946	5.2.3 Télécharger	Mettre à jour en version 2.4.1	6.8
	WordPress de version antérieure à 5.2.3 a un problème de vérification des adresses URL dans wp_kses_bad_protocol_once dans le fichier wp-includes / kses.php. Ce qui pourrait entraîner des attaques de type cross-site scripting (XSS).	11/09/2019	CVE-2019-16222		Mettre à jour en version 5.2.3	4.3
Vulnérabilité dans wondercms	Une vulnérabilité de type Directory traversal dans WonderCMS 2.6.0 et antérieures permettrait à des attaquants distants de supprimer des fichiers arbitraires via des vecteurs non spécifiés.	12/09/2019	CVE-2019-5956	2.7.0 Télécharger	Mettre à jour le CMS	7.5

II.2 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans adobe flash_player	Une vulnérabilité de type Same Origin Method Execution a été découverte dans Adobe Flash Player. Une exploitation réussie pourrait conduire à l'exécution de code arbitraire. Les versions affectées sont : • 32.0.0.238 et antérieures • 32.0.0.207 et antérieures	12/09/2019	CVE-2019-8069	32.0.0.255 Télécharger	Effectuer une mise à jour en version 3.0.0.255 ou ultérieure	10.0
Vulnérabilité dans libreoffice	Il a été découvert que le correctif pour LibreOffice de relative à la vulnérabilité de référence CVE-2019-9852 n'est pas complet.	13/09/2019	CVE-2019-9854	6.3.2 Télécharger	Mettre à jour en version 6.2.7 ou 6.3.2 ou ultérieure	7.5
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été corrigées dans les produits Microsoft. Elles permettent à un attaquant de provoquer un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et un déni de service.	11/09/2019	CVE-2019-1305	-	Effectuez une mise à jour via Windows Update	10.0

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 atteinte à la confidentialité des données, une élévation de privilèges, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	11/09/2019	CVE-2019-1297	2019	Mettre à jour le système via Windows Update	7.7
Vulnérabilité dans Microsoft .Net.	De multiples vulnérabilités ont été corrigées dans Microsoft .Net. Elles permettent à un attaquant de provoquer une élévation de privilèges et un déni de service.	11/09/2019	CVE-2019-1302	-	Mettre à jour le système via Windows Update	8.3
Vulnérabilité dans telegram	La fonction "supprimer pour" de Telegram de version antérieure à 5.11 sur Android ne supprime pas les fichiers multimédias partagés du répertoire Images de Telegram. En d'autres termes, une interface utilisateur potentiellement trompeuse indique qu'un expéditeur peut supprimer la copie d'un destinataire d'une image précédemment envoyée (analogue à la fonctionnalité prise en charge dans laquelle un expéditeur peut supprimer la copie d'un destinataire d'un message envoyé précédemment).	11/09/2019	CVE-2019-16248	5.11	Mettre à jour l'application	5.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans exchange_server	Une vulnérabilité de type déni de service existe dans le logiciel Microsoft Exchange Server due à une gestion incorrecte les objets en mémoire. Alias 'Microsoft Exchange Denial of Service Vulnerability'.	11/09/2019	CVE-2019-1233		Mettre à jour le système via Windows Update	7.8
Vulnérabilité dans alfresco	L'application Alfresco Share Community Edition est vulnérable à une attaque Open Redirect via une requête POST spécialement construite. En manipulant les paramètres du POST, un attaquant peut rediriger une victime vers un site Web malveillant via n'importe quel protocole souhaité. Les versions affectées sont les suivantes : Versions antérieures à 5.2.6, 6.0.N et 6.1.N	06/09/2019	CVE-2019-14223	6.1 Télécharger	Mettre à jour l'application	5.8
Vulnérabilité dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service à distance Les systèmes infectés sont les suivants : • Wireshark versions antérieures à 2.6.11 • Wireshark versions 3.0.x antérieures à 3.0.4	12/09/2019	-	3.0.5 Télécharger	Veuillez-vous referez au Bulletin de sécurité de l'éditeur https://www.wireshark.org/security/wnpa-sec-2019-21.html	10.0

III. ACTUALITÉS

1. Des centaines de milliers de trackers GPS peuvent être piratés à distance et tout dire de vos vies

Disponibles sur Amazon, eBay ou Alibaba, les trackers GPS se démocratisent de plus en plus. Pour quelques dizaines d'euros, il est désormais possible d'avoir un mouchard made in China qui vous permet de surveiller les déplacements de votre enfant, votre chien ou votre voiture. Le chercheur en sécurité Martin Hron d'Avast s'est penché sur le sujet et a découvert que bon nombre de ces appareils s'appuient en fait sur la même plate-forme technique et que celle-ci n'apporte quasiment aucune sécurité.

https://www.01net.com/actualites/des-centaines-de-milliers-de-trackers-gps-peuvent-etre-pirates-a-distance-et-tout-dire-de-vos-vies-1762531.html

2. Apple contre-attaque après les révélations de Google sur les piratages d'iPhone

Ce n'est pas une réaction à chaud, mais un message distillé lentement, à froid. Apple vient de publier une mise au point sur une révélation faite par Google il y a un peu plus d'une semaine. Le chercheur en sécurité Ian Beer de l'équipe Project Zero avait en effet détaillé une campagne de cybersurveillance très sophistiquée, mise en œuvre au travers d'une poignée de sites web piégés et ciblant des « milliers » d'utilisateurs iPhone « chaque semaine ».

https://www.01net.com/actualites/apple-contre-attaque-apres-les-revelations-de-google-sur-les-piratages-d-iphone-1764080.html

3. Vos photos Instagram et Facebook ne sont pas aussi privées que vous l'imaginez

Si vous êtes soucieux de votre vie privée, vous disposez peut-être d'un compte Instagram privé, où les photos et vidéos ne sont accessibles qu'aux personnes approuvées. Et sur Facebook, vous avez peut-être créé divers groupes d'amis pour limiter la visibilité de vos publications. Vous pensez être tranquille ? Pas de chance, les contenus multimédias partagés au travers de ces flux ne sont pas si verrouillés que cela.

https://www.01net.com/actualites/vos-photos-instagram-et-facebook-ne-sont-pas-aussi-privees-que-vous-l-imaginez-1764579.html

4. Une énorme faille dans les puces Intel Xeon permet d'espionner des ordinateurs à distance

Une faille spectaculaire dans un des caches des processeurs Intel Xeon permet de voler des informations sensibles. Un risque qui touche aussi bien les entreprises au travers de leurs datacenters que les utilisateurs de plates-formes cloud.

https://www.01net.com/actualites/une-enorme-faille-dans-les-puces-intel-xeon-permet-d-espionner-des-ordinateurs-a-distance-1766163.html

5. L'Arnaque au trading de cryptomonnaie est de retour

Il n'aura pas fallu bien longtemps pour que les escrocs spécialisés dans le trading de cryptomonnaie reviennent sur le devant de la scène. Après avoir usurpé le chanteur Booba, c'est au tour du patron de la société Iliad, Xavier Niel, d'en faire les frais. Face à ce genre de publicités...

https://www.zataz.com/larnaque-au-trading-de-cryptomonnaie-est-de-retour/

6. Piratage de webcam : un escroc français arrêté par les autorités

Depuis avril 2018, ZATAZ vous alerte de ces courriels vous annonçant le piratage de votre ordinateur et de votre webcam. Le « pseudo » pirate vous menace de diffuser des vidéos intimes. En échange de son silence, il est réclamé une certaine somme d'argent. Plusieurs dizaines d'escrocs et plusieurs centaines de versions de ces courriels parcourent les Internet depuis des mois.

https://www.zataz.com/piratage-de-webcam-un-escroc-francais-arrete-par-les-autorites/

7. Mémoire : Un pirate arrêté après avoir appris par cœur plus de 1 000 numéros de CB

Mémoire de Ninja ! Yusuke Taniguchi, un japonais de 34 ans, vient d'être appréhendé par la police nippone après avoir exploité plusieurs centaines de données bancaires qu'il avait piratées. Ici, pas de phishing, de logiciel espion. Yusuke a utilisé sa mémoire. Il a retenu, après les avoir lu, plus de 1 300 chiffres inscrits sur les cartes bancaires.

https://www.zataz.com/memoire-un-pirate-arrete-apres-avoir-appris-par-coeur-plus-de-1-000-numeros-de-cb/

8. Selon le FBI, les attaques BEC auraient coûté 26 milliards de dollars aux entreprises

Plus de 99% des cyberattaques requièrent une action humaine pour se propager. Les attaques BEC reposent sur l'engagement des individus et les cybercriminels s'appuient sur la psychologie humaine en demandant des réponses urgentes à des sollicitations pour des virements ou l'envoi de données confidentielles, simulant souvent un besoin commercial immédiat mais fictif.

https://www.undernews.fr/reseau-securite/selon-le-fbi-les-attaques-bec-auraient-coute-26-milliards-de-dollars-aux-entreprises.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**.