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 Décembre 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	Une vulnérabilité a été découverte dans Google Chrome. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : Google Chrome versions antérieures à 71.0.3578.98 sur Windows, Mac et Linux	13/12/2018	CVE-2017-17481	70.0.3578.98 Télécharger	Effectuez une mise à jour du navigateur	10.0
Vulnérabilité dans Mozilla Firefox ESR	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données. Les versions concernées sont les suivantes : Mozilla Firefox ESR de versions antérieures à la version 60.3	12/12/2018	CVE-2018-18498	60.4 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans IE et Edge	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une exécution de code à distance.	12/12/2018	CVE-2018-8629	-	Mettre à jour le système via Windows Update	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité les systèmes infectés sont les suivants : Ubuntu 18.04 LTS	04/12/2018	CVE-2017-18653	4.19.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3835-1/	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 un problème de sécurité non spécifié par l'éditeur, un déni de service à distance et un déni de service. Les systèmes infectés sont les suivants : SUSE Linux Enterprise Module pour Public Cloud 15Red Hat Enterprise Linux for Real Time for NFV 7 x86_64	04/12/2018	CVE-2017-18710	4.19.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20183961-1/	10.0

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 élévation de privilèges, une exécution de code à distance, une usurpation d'identité et un déni de service.	13/12/2018	CVE-2018-8637	-	Mettre à jour le système via Windows Update	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Wordpress	De multiples vulnérabilités ont été découvertes dans WordPress. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : WordPress versions antérieures à 5.0.1	13/12/2018	-	5.0.1 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs. https://wordpress.org/news/2018/12/wordpress-5-0-1-security-release/	6.4

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	De multiples vulnérabilités ont été corrigées dans Microsoft .Net. Elles permettent à un attaquant de provoquer un déni de service et une exécution de code à distance. Les versions affectées sont les suivants : Microsoft .NET Framework 4.7.2	12/12/2018	CVE-2018-8540	4.7.2	Effectuez une mise à jour du système Windows Update	4.1
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 atteinte à la confidentialité des données, une exécution de code à distance et une usurpation d'identité.	12/12/2018	CVE-2018-8650		Veuillez-vous référer au guide de sécurité https://portal.msrc.microsoft.com/fr-FR/security-guidance	4.5

Vulnérabilité dans Adobe Acrobat et Reader	De multiples vulnérabilités ont été découvertes dans Adobe Acrobat et Reader. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes affectés sont les suivants : Acrobat Reader DC versions antérieures à 2019.010.20064 sur Windows et macOS	12/12/2018	CVE-2018-19717	2019.010.20064 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/acrobat/apsb18-41.html	7.8
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, un déni de service à distance et un contournement de la politique de sécurité.	11/12/2018	CVE-2018-1900	9.0.5.0 Contacter IBM	Effectuez une mise à jour du système	2.1
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 et une exécution de code arbitraire à distance. PHP versions 7.x antérieures à 7.3.0	07/12/2018	CVE-2018-19158	7.3.0 Télécharger	Effectuez une mise à jour	4.3

III. ACTUALITÉS

1. Les photos de 68 millions d'utilisateurs de Facebook ont fuité à cause d'un bug

« Veuillez nous excuser pour la gêne occasionnée », écrit Facebook une nouvelle fois sur son site. Le réseau social vient en effet de révéler un problème dans ses fonctions de partage de données. Dans une note de blog, il indique avoir trouvé un bug dans son interface de programmation qui autorisait des applications tierces, qui avaient déjà le droit d'accéder aux photos du fil d'actualité, de mettre également la main sur des photos qui leur étaient interdites. Par exemple les photos publiées sur Facebook Stories ou Facebook Marketplace.

https://www.01net.com/actualites/facebook-les-photos-de-68-millions-d-utilisateurs-ont-fuite-a-cause-d-un-bug-1590209.html

2. Le pire mot de passe du monde

Il y a des choses qui ne semblent jamais changer. C'est le cas, par exemple, des mots de passe les plus populaires. La société SplashData a analysé plus de 5 millions de mots de passe qui ont fuité sur Internet cette année et publié un classement des 25 codes secrets les plus utilisés. Pas de surprise : « 123456 » et « password » occupent toujours respectivement la première et deuxième place. Tous les autres sont bien connus aussi. On retrouve ainsi les fameux « iloveyou », « welcome », « admin », « qwerty » ou sa variante « qwerty123 ».

https://www.01net.com/actualites/123456-encore-et-toujours-le-pire-mot-de-passe-du-monde-1588393.html

3. Microsoft reçoit vos données même si vous ne le voulez pas

Depuis quelques jours, un imbroglio autour de l'historique des activités agite le forum Reddit. Certains utilisateurs ont remarqué que, lorsqu'ils désactivaient l'option « Envoyer l'historique des activités à Microsoft », l'éditeur les reçoit quand même. Cette case à décocher se trouve dans « Paramètres -> Confidentialité -> Historique des activités ».

https://www.01net.com/actualites/windows-10-microsoft-recoit-vos-donnees-d-activite-meme-si-vous-ne-le-voulez-pas-1587584.html

4. Ces pirates qui ne s'attaquent qu'aux infrastructures critiques

Les chercheurs en sécurité de McAfee viennent de détecter des actions de cyberespionnage au niveau mondial ciblant des entreprises de secteurs stratégiques comme le nucléaire, la défense, l'énergie ou la finance. Baptisée « Opération Sharpshooter », cette campagne a visé au moins 87 entreprises dans 31 pays. Les victimes sont principalement situées aux Etats-Unis, mais il y en a également en Europe, et notamment en France. « La plupart des organisations ciblées sont anglophones ou disposent d'une filiale anglophone », précise McAfee dans une note de blog.

https://www.01net.com/actualites/defense-nucleaire-telecoms-ces-pirates-s-attaquent-aux-infrastructures-critiques-de-31-pays-1587339.html

5. Des Hackers chinois derrière le vol des données des hôtels Marriott

C'est à la fois une bonne et une mauvaise nouvelle. Selon The New York Times (NYT), les données des 500 millions de comptes, qui ont été siphonnés dans les bases de données de la filiale Starwood du groupe Marriott, n'auraient pas été récupérées par des cybercriminels. Ouf. Ce serait le ministère de la Sécurité de l'Etat, l'un des services de renseignement de la Chine. Ah... Le risque de fraude bancaire s'en trouve limité pour les personnes concernées.

https://www.01net.com/actualites/des-hackers-chinois-seraient-derriere-le-vol-des-donnees-de-500-millions-de-comptes-des-hotels-marriott-1586553.html

6. Les malwares se multiplient sous Linux

Si Windows reste la cible principale des pirates, cela ne veut pas dire que les autres systèmes d'exploitation ne sont pas également victimes de malwares. Ils le sont, mais à un degré moindre, c'est pourquoi ce phénomène passe souvent inaperçu. Mais quand on se focalise sur l'un de ces systèmes, on trouve assez rapidement quelque chose. C'est ce qui s'est produit pour les chercheurs en sécurité d'Eset. En analysant la mécanique du botnet Windigo, ils ont découvert l'existence d'un vaste arsenal de portes dérobées qui, jusqu'à présent, avaient échappé à l'attention des experts en sécurité.

https://www.01net.com/actualites/sous-linux-aussi-les-malwares-se-multiplient-1585851.html

7. La 5G n'est pas encore là mais on y découvre beaucoup de vulnérabilités

Ceux qui pensent que la sécurité sera totalement béton avec la 5G vont être déçus. Un groupe de chercheurs viennent de révéler une faille dans le design du protocole Authentication and Key Agreement (AKA), qui assure l'authentification de l'abonné et l'échange des clés pour chiffrer le trafic. Ce protocole existait déjà pour la 3G et la 4G. Pour la 5G, certains mécanismes cryptographiques ont été renforcés, notamment afin d'empêcher les « IMSI Catcher », ces fausses stations de base, de détecter la présence de certaines personnes dans une zone donnée. Ce qui était plutôt une bonne idée.

https://www.01net.com/actualites/la-5g-n-est-pas-encore-la-mais-a-deja-une-grosse-faille-de-securite-1583854.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**.