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 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	De multiples vulnérabilités ont été découvertes dans Google Chrome. Elles permettent 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 71.0.3578.94 (Platform version: 11151.59.0)	18/12/2018		71.0.3578.94 Télécharger	Effectuez une mise à jour du navigateur	10.0
Vulnérabilité dans IE	Une vulnérabilité a été découverte dans Microsoft Internet Explorer. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.	20/12/2018	CVE-2018-8653	-	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. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : Ubuntu 18.04 LTS Ubuntu 18.10	20/12/2018	CVE-2017-18710	4.20 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3846-1/	10.0
Vulnérabilité dans le noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et une élévation de privilèges. Les systèmes infectés sont les suivants : SUSE Linux Enterprise Server 12-SP1-LTSS, SUSE Linux Enterprise Live Patching 12-SP3	18/12/2018	CVE-2017-9568	4.20 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20184154-1/	10.0

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Fin de support de de la version 5 de PHP	The PHP GROUP » annonce la fin de support des versions 5.6.x de PHP à partir du 31 Décembre 2018. Après cette date toutes les versions 5 de PHP ne recevront plus les mises à jour et les correctifs de sécurité. Il est recommandé aux différents organismes de planifier la migration de leurs applications web vers une des versions supportées de PHP. Il est à noter que sans mises à jour de sécurité pour ce composant, vos applications web deviennent vulnérables à une panoplie d'attaques qui peuvent cibler les informations contenues dans ces applications ou être utilisés comme porte d'entrée pour attaquer d'autres éléments de votre système d'information. Pour plus d'informations sur ce sujet veuillez-vous référer à ce bulletin d'information de PHP : □ http://php.net/supported-versions.php					
Vulnérabilité dans Adobe Acrobat et Reader	Adobe a publié une mise à jour qui permet de corriger plusieurs vulnérabilités dans certaines versions de son produit Adobe Acrobat et Adobe Reader. Certaines de ces vulnérabilités sont critiques et leur exploitation peut permettre à un attaquant l'exécution de code arbitraire, l'accès à des informations confidentielles ou l'élévation de privilèges. Les systèmes affectés sont les suivants : Acrobat Reader DC versions antérieures à 2019.010.20081 sur Windows et macOS	17/12/2018	CVE-2018-19720	2019.010.20081 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 Tenable Nessus	De multiples vulnérabilités ont été découvertes dans Tenable Nessus. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : Nessus versions 8.1.0 et antérieures	21/12/2018	CVE-2018-5407	8.1.1 Télécharger	Effectuez une mise à jour de l'application	2.1
Vulnérabilité dans Cisco ASA	Une vulnérabilité a été découverte dans le logiciel de l'équipement Cisco ASA. Elle permet à un attaquant de provoquer une élévation de privilèges	20/12/2018	CVE-2018-15465	Contacter CISCO	Veuillez-vous référer au guide de sécurité https ://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20181219-asa-privesc	4.3
Vulnérabilité dans VMware vRealize Operations	Une vulnérabilité a été découverte dans VMware vRealize Operations. Elle permet à un attaquant de provoquer une élévation de privilèges.	18/12/2018	CVE-2018-6978	Contacter VMware	Veuillez-vous référer au guide de sécurité https://www.vmware.com/security/advisories/VMSA-2018-0031.html	6.4

Vulnérabilité dans Samba	Plusieurs vulnérabilités affectant plusieurs versions de Samba ont été corrigées. L'exploitation de ces vulnérabilités peut permettre à un attaquant de causer un déni de service. Les systèmes infectés sont les suivants : Paquets Samba versions antérieures à la version 2:4.2.14+dfsg-0+deb8u11.	18/12/2018	CVE-2018-16851	4.9.4 Télécharger	Veuillez-vous référer au guide de sécurité https://lists.debian.org/debian-lts-announce/2018/12/msg00005.html	2.1

III. ACTUALITÉS

1. Des hackers cassent la reconnaissance veineuse

Considérée comme particulièrement sécurisée, la reconnaissance veineuse peut être piégée avec une fausse main ou un faux doigt, moulé en cire d'abeille. Quelques dizaines de minutes suffisent pour créer un tel dispositif.

https://www.01net.com/actualites/des-hackers-ont-casse-l-authentification-par-reconnaissance-veineuse-1599403.html

2. Wannacry continue d'infecter des centaines de milliers de pc dans le monde

Le vendredi 12 mai 2017, une gigantesque attaque informatique avait frappé le monde. Des pirates – probablement nord-coréens – avaient lâché sur Internet un ransomware ultravirulent baptisé WannaCry. Il s'appuyait sur des outils volés à la NSA pour se diffuser à la vitesse de l'éclair. En quelques heures, des centaines de milliers d'ordinateurs Windows ont cessé de fonctionner : PC de bureau, panneaux publicitaires, écrans de contrôle ferroviaires, bornes d'informations, guichets automatiques, etc.

https://www.01net.com/actualites/le-ver-wannacry-continue-d-infecter-des-centaines-de-milliers-de-pc-dans-le-monde-1598994.html

3. Des failles de sécurité dans plus de 16.000 orange livebox

Mauvaise surprise de fin d'année pour les abonnés d'Orange España. Il y a quelques jours, le chercheur en sécurité Troy Mursch a détecté de mystérieux scans réseaux sur des modems ADSL Orange Livebox. Ces scans effectuaient des requêtes HTTP/GET sur un script CGI intégré dans ces boîtiers et accessibles depuis Internet. En réponse, l'attaquant obtient le nom et le mot de passe du réseau Wi-Fi de la Livebox en question.

https://www.01net.com/actualites/des-failles-de-securite-dans-plus-de-16-000-orange-livebox-1598862.html

4. Impossible de cacher sa position à Facebook

Les contrôles de localisation fournis par Facebook donnent l'illusion à une personne de contrôler les données relatives à son expérience publicitaire, et non le contrôle réel. De plus, Facebook fait de fausses déclarations sur l'effet de ces contrôles. » Cette déclaration – qui a le mérite d'être claire – a été faite par Aleksandra Korolova, professeur assistante d'informatique à l'université de Californie du Sud

https://www.01net.com/actualites/pourquoi-il-est-impossible-de-cacher-votre-position-geographique-a-facebook-1592696.html

5. Innombrables failles de sécurité de la défense antimissile américaine

Absence de chiffrement, manque d'authentification, systèmes non patchés depuis des années… La sécurité informatique de la défense antimissile des Etats-Unis n'est pas au niveau de sa valeur stratégique pour ce pays.

https://www.01net.com/actualites/les-innombrables-failles-de-securite-de-la-defense-antimissile-americaine-1590556.html

6. Une importante attaque informatique vise des médias aux USA

Les journaux américains le Los Angeles Times, le Chicago Tribune ou encore le Baltimore Sun perturbés par un ransomware. Une attaque informatique a empêché les journaux d'éditer les avis nécrologiques et les petites annonces.

https://www.zataz.com/une-attaque-informatique-vise-plusieurs-media-usa-et-bloque-certains-articles-des-journaux-papier/

7. Le FBI met fin aux activités de 15 services de DDoS

Le ministère américain de la Justice vient d'annoncer que le FBI avait saisi les noms de domaines de 15 sites Web de « DDoS contre rétribution » et avait mis en accusation trois personnes qui exploitaient certains de ces services. Les services DDoS contre abonnement, ou « Booter » / « Stresser », louent l'accès à un réseau de périphériques infectés (botnet) à n'importe quel internaute (même le moins expérimenté en technologies), qui peut ensuite être utilisé contre n'importe quelle cible pour lancer un déni de service distribué pouvant limiter l'accès voir l'empêcher totalement selon la puissance de l'attaque.

https://www.undernews.fr/hacking-hacktivisme/le-fbi-met-fin-aux-activites-de-15-services-de-ddos.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**.