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 Novembre 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	Google vient de publier une mise à jour de sécurité qui permet de corriger une vulnérabilité dans le navigateur Google chrome et le système d'exploitation Chrome OS. L'exploitation de cette vulnérabilité peut permettre à un attaquant de causer des problèmes non spécifiés par l'éditeur. Les systèmes infectés sont les suivants : Google Chrome versions antérieures à 70.0.3538.110 sur Windows, Mac et Linux	22/11/2018		70.0.3538.110 Télécharger	Effectuez une mise à jour du navigateur	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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, un déni de service et une atteinte à la confidentialité des données. les systèmes infectés sont les suivants : SUSE Linux Enterprise Server 12-SP4	29/11/2018	CVE-2017-18710	4.19.6 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20183934-1/	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 et un déni de service. Les systèmes infectés sont les suivants : Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64	27/11/2018	CVE-2017-14646	4.19.6 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2018:3666	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Magento	L'équipe de sécurité de Magento annonce la correction de plusieurs vulnérabilités au niveau de certaines versions du CMS Magento. L'exploitation de ces vulnérabilités peut permettre l'exécution de code arbitraire à distance l'élévation de privilèges ou l'accès à des données confidentielles. Les systèmes affectés sont les suivants : Magento Commerce versions 2.2.x antérieures à la version 2.3.0	30/11/2018	-	2.3.0 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs. https://magento.com/security/patches/magento-2.2.7-and-2.1.16-security-update	6.4

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Samba	De multiples vulnérabilités ont été découvertes dans Samba. Elles permettent à un attaquant de provoquer un déni de service à distance et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : Samba versions 4.9.x antérieures à 4.9.3	27/11/2018	CVE-2018-16857	4.9.3 Contacter Samba	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs. https://www.samba.org/samba/security/CVE-2018-16857.html	9.2
Vulnérabilité dans Symantec	Symantec annonce la publication de mises à jour qui corrigent plusieurs vulnérabilités au niveau de certains de ses produits. L'exploitation de ces vulnérabilités peut permettre à un attaquant le contournement de la politique de sécurité.	30/11/2018	CVE-2018-12245	Contacter Symantec	Veuillez-vous référer au guide de sécurité https://support.symantec.com/content/unifiedweb/en_US/article.SYMSA1468.html	8.7

Vulnérabilité dans Adobe Flash Player	Adobe vient de publier des mises à jour qui permettent de corriger une vulnérabilité critique dans son produit Adobe Flash Player. L'exploitation de cette vulnérabilité peut permettre à un attaquant l'exécution de code arbitraire les systèmes affectés sont les suivants : • Adobe Flash Player Desktop Runtime versions antérieures à 31.0.0.148 sur Windows, macOS • Adobe Flash Player pour Google Chrome versions antérieures à 31.0.0.148 sur Windows, macOS, Linux et Chrome OS	27/11/2018	CVE-2018-15981	31.0.0.148 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/flash-player/apsb18-44.html	7.8
Vulnérabilité dans les produits VMware	Vmware a publié la correction d'une vulnérabilité affectant Vmware Worksation et Fusion. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code arbitraire. Les systèmes infectés sont les suivants : Workstation versions 15.x antérieures à 15.0.2	23/11/2018	CVE-2018-6980	Contacter VMware	Effectuez une mise à jour	4.3

Vulnérabilité dans les produits XEN	De multiples vulnérabilités ont été découvertes dans Xen. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges. Tous Les systèmes sans correctifs sont vulnérables.	21/11/2018	-	4.8.x Télécharger	Effectuez une mise à jour	4.3
Vulnérabilité dans Moodle	Une vulnérabilité a été découverte dans Moodle. Elle permet à un attaquant de provoquer une injection de requêtes illégitimes par rebond (CSRF). Toutes les versions antérieures à Moodle version 3.5.3 sont infectées.	19/11/2018	CVE-2018-16854	3.5.3 Télécharger	Effectuez une mise à jour	7.3

III. ACTUALITÉS

1. DELL réinitialise tous les password de ses clients

Si vous êtes un client de Dell, la prochaine fois que vous allez vous connecter à votre compte client, ne soyez pas surpris de devoir changer votre mot de passe. Le fabricant vient de tous les réinitialiser, par mesure de précaution. En effet, le 9 novembre dernier, il a détecté dans ses réseaux la présence de pirates qui cherchaient à subtiliser les noms, les adresses e-mail et les empreintes de mots de passe de sa base de données clients. Les données de cartes bancaires n'ont pas été ciblées.

https://www.01net.com/actualites/victime-de-piratage-dell-reinitialise-tous-les-mots-de-passe-de-ses-clients-1577172.html

2. Fraude publicitaire : le gang 3VE démantelé

Google, WhiteOps et une dizaine d'autres acteurs du numérique ont assisté le FBI dans le démantèlement d'une gigantesque fraude publicitaire qui aurait généré plus de 36 millions de dollars de revenus entre 2014 et 2018. Huit personnes d'origine russe et kazakh ont été mises en accusation par le Ministère de la justice américaine. Trois d'entre eux ont d'ores et déjà été arrêtés et attendent leur extradition vers les Etats-Unis. Ils croupissent actuellement dans des prisons en Malaisie, Estonie et Bulgarie. Les autres sont en cavale.

https://www.01net.com/actualites/fraude-publicitaire-demantelement-de-3ve-un-gang-de-pirates-aux-techniques-ultrasophistiquees-1576355.html

3. Des applis frauduleuses qui détournent des millions

Sur Internet, tout peut se monnayer, y compris l'installation d'applications mobiles. Mais les circuits de rémunération sont loin d'être sécurisés, comme vient de le montrer BuzzFeed. Kochava, une société spécialisée dans le Web marketing, aurait ainsi détecté huit applications mobiles qui procèdent en douce à une fraude publicitaire ayant généré plusieurs millions de dollars.

https://www.01net.com/actualites/comment-des-appli-frauduleuses-detournent-des-millions-de-dollars-en-publicite-sur-android-1575728.html

4. Black Friday attention aux cyber arnaques

Une avalanche de promotions en ligne, des acheteurs heureux qui font chauffer leurs cartes bancaires, des boutiques qui croulent sous le nombre de connexions par minute… C'est aujourd'hui la journée du « Black Friday » et tout semble indiquer qu'elle va battre tous les records de vente

.https://www.01net.com/actualites/black-friday-attention-aux-cyberarnaques-car-les-pirates-sont-de-sortie-1572703.html

5. Un simple code JavaScript suffit pour savoir quels sites vous visitez

Pour surfer de manière anonyme sur la Toile, utiliser le navigateur Tor est un bon début, mais ce n'est pas forcément suffisant. Il est également judicieux de fermer tous les autres navigateurs éventuellement ouverts, car ces derniers pourraient révéler vos pérégrinations. Un groupe de chercheurs en sécurité vient en effet de découvrir qu'il était possible de surveiller la navigation web d'un utilisateur en observant l'utilisation de la mémoire cache de l'ordinateur depuis un simple code JavaScript. En d'autres termes, il suffit d'ouvrir un site hébergeant un tel code malveillant pour que cet onglet de navigation soit capable d'espionner tous les autres onglets qui tournent sur la même machine, qu'ils appartiennent au même navigateur ou non. Et y compris ceux du navigateur Tor.

https://www.01net.com/actualites/un-code-javascript-suffit-pour-savoir-quels-sites-web-vous-visitez-1572207.html

6. Quinze minutes pour pirater un distributeur de billets de banque

Les cyberbraqueurs de banques n'ont pas de soucis à se faire quant à leur employabilité. Une récente analyse de sécurité réalisée par Positive Technologies sur 26 distributeurs de billets (DAB) montre que ces appareils sont tellement peu sécurisés qu'il suffit généralement d'un quart d'heure pour en prendre le contrôle et les dévaliser, sous certaines conditions. Les marques testées sont NCR, Diebold Nixdorf et GRGBanking.

https://www.01net.com/actualites/les-distributeurs-de-billets-de-banques-toujours-autant-truffees-de-failles-1570620.html

7. Plusieurs botnet interrompus suite à une opération anti-fraude

Internet a remporté une grande victoire, après le démantèlement par le FBI, d'une opération de cybercriminalité d'envergure, menée depuis plusieurs années. Les pirates utilisaient des botnets pour manipuler le trafic internet. En mobilisant 1,7 million d'adresses IP, ils avaient pu générer près de 30 millions de dollars en revenus publicitaires frauduleux. F-Secure a participé à l'opération de démantèlement en fournissant des informations sur les campagnes de malware et les botnets servant à l'opération.

https://www.undernews.fr/hacking-hacktivisme/plusieurs-botnets-interrompus-suite-a-une-operation-anti-fraude.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**.