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 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 Mozilla Firefox ESR	Mozilla Foundation annonce la disponibilité d'une mise à jour de sécurité permettant de corriger plusieurs vulnérabilités dans Mozilla Thunderbird ESR. L'exploitation de ces vulnérabilités peut permettre à un attaquant l'exécution de code arbitraire, le contournement de la politique de sécurité ou le déni de service. Les versions concernées sont les suivantes : Mozilla Firefox ESR de versions antérieures à la version 60.3	01/11/2018	CVE-2018-12393	60.3 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans IE et Edge	Plusieurs vulnérabilités ont été corrigées au niveau des deux navigateurs de Microsoft ; Internet Explorer et Edge. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant l'accès à des données confidentielles, l'exécution de code arbitraire ou le contournement de la politique de sécurité	14/11/2018	CVE-2018-8588	-	Mettre à jour le système via Windows Update	10.0

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 70.0.3538.102 sur Windows, Mac et Linux	12/11/2018	CVE-2018-17477	70.0.3538.102 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 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.	13/11/2018	CVE-2018-8605	-	Mettre à jour le système via Windows Update	10.0

Vulnérabilité dans Juniper Junos OS	De multiples vulnérabilités ont été découvertes dans Juniper Junos OS. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à l'intégrité des données.	14/11/2018	CVE-2017-7185	Contacter Juniper	Veuillez-vous référer au Bulletin de sécurité https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10898&cat=SIRT_1&actp=LIST	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 déni de service à distance, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.	12/11/2018	CVE-2017-16658	4.19.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2018/suse-su-20183689-1/	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 à distance.	07/11/2018	CVE-2017-18344	4.19.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2018:3459	10.0
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 à distance, un déni de service à distance et une atteinte à la confidentialité des données	15/11/2018	CVE-2017-9588	4.19.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3819-1/	10.0

II.3 SERVEURS WEB

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les serveurs Nginx	De multiples vulnérabilités critiques ont été corrigées au niveau du serveur web Nginx. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant l'accès à des données confidentielles ou le déni de service. Les systèmes affectés sont les suivants : Nginx versions antérieures à 1.15.6 et 1.14.1	09/11/2018	CVE-2018-16845	Contacter Nginx	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs. http://mailman.nginx.org/pipermail/nginx-announce/2018/000220.html?_ga=2.53242600.1560703116.1541576907-1155548486.1533906360	9.2

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	Une vulnérabilité a été corrigée dans Microsoft .Net. Elle permet à un attaquant de provoquer un contournement de la fonctionnalité de sécurité. Les versions affectées sont les suivants : .NET Core 2.1	14/11/2018	CVE-2018-8416	2.1	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 atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et un déni de service.	14/11/2018	CVE-2018-8582		Veuillez-vous référer au guide de sécurité https://portal.msrc.microsoft.com/fr-FR/security-guidance	4.5
Vulnérabilité dans Adobe Flash Player	Une vulnérabilité a été découverte dans Adobe Flash Player. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. 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	14/11/2018	CVE-2018-15978	31.0.0.148 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/flash-player/apsb18-39.html	7.8

Vulnérabilité dans les produits VMware	Une vulnérabilité a été découverte dans VMware vRealize Log Insight. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes infectés sont les suivants : VMware vRealize Log Insight (vRLI) versions 4.7.x antérieures à 4.7.1	14/11/2018	CVE-2018-6980	Contacter VMware	Effectuez une mise à jour	6.2
Vulnérabilité dans VirtualBox	Un chercheur en sécurité a publié sur la plateforme GitHub des détails sur une vulnérabilité de type "zero-day" affectant VirtualBox. Selon les informations publiées sur GitHub cette vulnérabilité peut permettre à un code malveillant de s'échapper de l'environnement virtuel, infecter la machine hôte et élever le privilège vers « Ring 3 privilege layer » qui permet d'exécuter la plupart des programmes utilisateurs. Le chercheur affirme que le "zero-day" affecte toutes les versions actuelles de VirtualBox, quel que soit le système d'exploitation hôte ou invité que l'utilisateur utilise ainsi que la configuration par défaut des machines virtuelles. **Solution** : Aucun patch ou mise à jour ne sont disponibles pour le moment. Cependant il est recommandé de : - Changer la carte réseau de la machine virtuelle à « PCnet » ou « Paravirtualized Network ». - Changer le mode réseau de la machine virtuelle de NAT vers un autre mode si la première recommandation est impossible à implémenter dans votre environnement. **Annexe :** https://github.com/MorteNoir1/virtualbox_e1000_0day VirtualBox 5.2.20 et toutes les versions antérieures sont concernées par cette vulnérabilité.					

III. Actualités

1. Les hackers russes sèment le chaos

Quand les cyberagents de la direction générale des renseignements de l'armée russe (Glavnoyé Razvédyvatel'noyé Oupravléniyé, GRU) passent à l'action, ils ne font pas toujours dans la dentelle. Parmi les dernières actions qui ont marqué les esprits figure une escapade rocambolesque à La Haye en avril dernier. Arrivée par avion, une équipe de quatre agents, tous dotés de passeports diplomatiques, a tenté de pirater le réseau informatique de l'Organisation pour l'interdiction des armes chimiques (OIAC).

https://www.01net.com/actualites/espionnage-sabotage-intox-comment-les-hackers-de-l-armee-russe-sement-le-chaos-1562952.html

2. Le chiffrement matériel des disques SSD pas fiable

Les chercheurs ont testé sept disques durs. Trois proviennent de Crucial (MX100, MX200, MX300) et quatre de Samsung (840 EVO SATA, 850 EVO SATA, T3 USB, T5 USB). Tous ces modèles sont vulnérables d'une manière ou d'une autre et permettent à un attaquant qui dispose d'un accès physique au disque de déchiffrer les données. En d'autres termes : si ce disque est volé ou perdu, rien n'empêchera une personne malveillante d'accéder à son contenu.

https://www.01net.com/actualites/pourquoi-le-chiffrement-materiel-des-disques-ssd-ne-vaut-souvent-pas-un-clou-1561226.html

3. Et si on pouvait pirater votre cerveau ?

A l'occasion d'une conférence organisée par Kaspersky Labs à Barcelone, Laurie Pycroft, chercheur à l'université d'Oxford dans le domaine de la neurochirurgie, explique que la modification de la mémoire est une technologie qui pourrait exister dans quelques dizaines d'années. Elle pourrait s'appuyer sur une évolution de la stimulation cérébrale profonde (Deep Brain Stimulation, DBS).

https://www.01net.com/actualites/et-si-l-on-pouvait-un-jour-pirater-votre-cerveau-1556169.html

4. Le ministre japonais chargé de la cyber sécurité n'a jamais utilisé un ordinateur

Le ministre japonais chargé de la cyber-sécurité a provoqué les rires mâtinés d'angoisse de l'opposition mercredi après avoir reconnu n'avoir jamais utilisé d'ordinateur dans sa vie professionnelle. Yoshitaka Sakurada, 68 ans, est le chef adjoint de l'unité de stratégie de sécurité informatique du gouvernement et également ministre des jeux Olympiques et Paralympiques, que Tokyo organise en 2020. Durant une session en commission parlementaire mercredi, il a reconnu sa lacune: "Depuis l'âge de 25 ans, j'ai toujours eu recours à mes employés ou secrétaires, donc je n'ai jamais utilisé d'ordinateur".

https://www.rtl.be/info/magazine/hi-tech/japon-le-ministre-charge-de-la-cyber-securite-n-a-jamais-utilise-d-ordinateur-1077344.aspx

5. Windows patches une faille 0day utilisée par des hackers

Posted on Author Cyber Security Review Microsoft released today its monthly roll-up of security patches known as Patch Tuesday. This month, the Redmond-based company has fixed 62 security flaws. Among the 62 fixes, there is also a fix for a zero-day vulnerability that was under active exploitation before today's patches were made available.....

https://cert.europa.eu/cert/moreclusteredition/en/brica-b4404f797a62e427c514d237d5de8791.20181113.en.html

6. Une faille WordPress permet l'accès à tout utilisateur

Another day, another critical WordPress plugin vulnerability. The popular AMP for WP plugin, which helps WordPress sites load faster on mobile browsers, has a privilege-escalation flaw that allows WordPress site users of any level to make administrative changes to a website.

https://threatpost.com/critical-wordpress-flaw-grants-admin-access-to-any-registered-site-user/139162/

7. L'armée américaine veut hacker les cerveaux de ses soldats

Cela ressemble à un mauvais épisode de la série X Files. La Darpa (Defense Advanced Research Projects Agency) réfléchit très sérieusement à hacker le cerveau de ses soldats depuis plusieurs années, comme l'explique longuement le site The Atlantic. Officiellement, les recherches en neurotechnologie de cette agence du département de la Défense se concentrent sur le maintien et la restauration physique des soldats. Mais elle poursuit aussi une mission beaucoup plus vaste et de longue haleine : libérer notre cerveau des limitations de notre corps en fusionnant l'homme et la machine. Un vrai rêve de Transhumanistes !

. https://www.01net.com/actualites/comment-l-armee-americaine-veut-hacker-le-cerveau-de-ses-soldats-1544602.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**.