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 Février 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 Google Chrome	De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : Google Chrome OS versions antérieures à 72.0.3626.97 (Platform version: 11316.123.0, 11316.123.1)	11/02/2019	–	72.0.3626.97 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 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 une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : Ubuntu 18.04 LTS, Ubuntu 16.04 LTS, Ubuntu 14.04 LTS, Ubuntu 12.04 ESM	05/02/2019	CVE-2018-20179	18.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/3878-3/	10.0
Vulnérabilité dans Google Chrome OS	De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : Google Chrome OS versions antérieures à 72.0.3626.97 (Platform version: 11316.123.0, 11316.123.1)	11/02/2019	–	72.0.3626.97 Contacter	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/02/stable-channel-update-for-chrome-os.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleChromeReleases+%28Google+Chrome+Releases%29	9.0

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, et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : SUSE Linux Enterprise Live Patching 12-SP4 SUSE Linux Enterprise Workstation Extension 15 SUSE Linux Enterprise Module pour Open Buildservice Development Tools 15	04/02/2019	CVE-2018-20169	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20190298-1/	10.0

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité de type Zero-day dans Microsoft Exchange	**Bilan de la vulnérabilité** : Microsoft a publié une mise à jour pour limiter l'exploitation d'une faille critique au niveau du Serveur Microsoft Exchange. L'exploitation de cette faille peut permette à un utilisateur malveillant disposant d'un compte exchange de réussir une élévation de privilèges et obtenir le droit Admin sur le Contrôleur de Domaine. Pour remédier à cette vulnérabilité, une politique de limitation pour EWSMaxSubscriptions peut être définie et appliquée avec la valeur zéro. Cela empêchera le serveur Exchange d'envoyer des notifications EWS et empêchera les applications clientes qui reposent sur les notifications EWS de fonctionner normalement. **Solution** : • Veuillez-vous référer au bulletin de sécurité Microsoft du 05 Février 2019 : • https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190007 • https://www.dgssi.gov.ma/fr/content/1935280119-vulnerabilite-de-type-zero-day-dansmicrosoft-exchange.html **Risque** : Elévation de privilèges ; Perte de contrôle du système affecté.					

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans LibreOffice	Une vulnérabilité a été découverte dans LibreOffice. Elle permet à un attaquant de provoquer une exécution de code arbitraire. Les systèmes affectés sont les suivants : LibreOffice versions antérieures à 6.0.7 et 6.1.3	08/02/2019	CVE-2018-16858	6.2.0 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.libreoffice.org/about-us/security/advisories/cve-2018-16858/	7.8
Vulnérabilité dans Nagios Core 4	Une vulnérabilité a été découverte dans Nagios Core 4. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Nagios versions antérieures à 4.4.3.	07/02/2019	CVE-2018-18245	4.4.3 Télécharger	Effectuez une mise à jour	5.1
Vulnérabilité dans les produits CISCO	Cisco a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités dans Cisco Webex et Cisco Meeting. Un attaquant pourrait exploiter ces vulnérabilités pour prendre le contrôle d'un système affecté et d'exécuter du code arbitraire à distance.	16/01/2019	CVE-2019-1639	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190123-webex-rce	5.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Apple	De multiples vulnérabilités ont été découvertes dans les produits Apple. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les produits affectés sont : iOS versions antérieures à 12.1.4 maxOS Mojave versions antérieures à 10.14.3 Shortcuts pour iOS versions antérieures à 2.1.3	08/02/2019	CVE-2019- 7290	12.1.4 Site web	Effectuez une mise à jour du système	5.6

III. ACTUALITÉS

1. Apple vient de corriger deux failles zéro day

La mise à jour 12.1.4 ne corrige pas seulement le fameux bug FaceTime, mais aussi deux failles critiques exploitées de manière active par les pirates. Ce qui est potentiellement plus grave. Si vous avez un iPhone ou un iPad, pensez à mettre à jour votre système d'exploitation dès que vous pourrez. Disponible depuis hier, la dernière mise à jour (iOS 12.1.4) colmate deux failles critiques qui sont d'ores et déjà exploitées de manière active par les pirates.

https://www.01net.com/actualites/mettez-a-jour-ios-apple-vient-de-corriger-deux-failles-zero-day-activementexploitees-par-des-pirates-1628919.html

2. L'ouverture d'un simple PNG peut suffire pour que vous soyez piratés

Google vient de corriger une faille critique dans Android qui peut être exploitée par le biais d'une simple image. Pour éviter tout risque de piratage, vérifiez que votre système est bien à jour. La bonne nouvelle, c'est que cette faille n'est pas exploitée par les pirates pour le moment. Mais ce n'est probablement qu'une question de temps. La première chose que les hackers malintentionnés font dès qu'un patch de ce calibre est publié, c'est de l'analyser par rétro-ingénierie pour retrouver le bug qui en est à l'origine. Il est donc vivement conseillé de mettre à jour son appareil.

https://www.01net.com/actualites/ouvrir-une-simple-image-png-suffit-pour-que-votre-smartphone-android-soit-pirate-1628850.html

3. Une faille critique dans Apple

Un chercheur en sécurité a révélé une faille zero-day dans le coffre-fort des mots de passe de macOS. Mais il ne veut pas transmettre les détails à Apple tant que celui-ci ne proposera pas de bug bounty. Une question de principe, selon lui. Linus Henze est plutôt du genre têtu. Ce chercheur en sécurité vient de trouver une faille critique dans le coffre-fort des mots de passe de macOS (« Keychain » alias « Trousseaux d'accès »).

https://www.01net.com/actualites/il-a-trouve-une-faille-critique-dans-macos-mais-ne-veut-pas-la-livrer-a-apple-1627943.html

4. Vous saurez bientôt à qui Facebook vend vos données

La plate-forme met en place un nouveau bouton permettant de connaître l'identité des agences ou développeurs qui vous ciblent publicitairement et s'ils ont téléchargé votre numéro de téléphone et adresse mail.

https://www.01net.com/actualites/vous-saurez-bientot-quelle-marque-a-recupere-vos-coordonnees-sur-facebook-1628023.html

5. Protéger vos passeports informatiques

Trois hommes ont organisé une vaste fraude qui, à coup de messages anxiogènes, consistait à inciter des internautes français à payer pour un faux service de dépannage informatique. Plus de 8 000 personnes sont tombées dans le panneau. Les pirates n'ont pas toujours le profil que l'on attend. Des suspects ont été interpellés et mis en examen la semaine dernière, dans le cadre d'une cyber-arnaque au faux support informatique qui a touché 8 000 français pour un préjudice de plus de deux millions d'euros. Il s'agit de trois hommes de 30 à 54 ans, chefs d'entreprise dans la région lyonnaise dans le secteur de l'assurance, comme le révèle Le Parisien. On est donc loin du cliché du cyberdélinquant avec gilet à capuche.

https://www.01net.com/actualites/ils-ont-soutire-deux-millions-d-euros-grace-a-un-faux-support-informatique-1626903.html

6. La chute du premier super Marché du dark web

Capturer Ross Ulbricht, le premier grand cyber-caïd de la drogue, n'a pas été une mince affaire. Les forces de l'ordre ont tâtonné pendant longtemps, multipliant les échecs. Voici le récit de cette enquête hors norme. Vous souvenez-vous de Ross Ulbricht ? Ce jeune homme américain plutôt propret a été le premier à fonder et opérer une énorme place de marché de la drogue sur le Dark Web. Baptisé « Silk Road », ce site a démarré en février 2011 et n'était accessible que par Tor Browser. Le site a fonctionné jusqu'à l'arrestation de son créateur en octobre 2013 et a brassé au final presque 10 millions de bitcoins. Par la suite, Ross Ulbricht a été condamné à la prison à vie.

https://www.01net.com/actualites/l-incroyable-enquete-qui-a-mene-a-la-chute-du-premier-supermarche-du-dark-web-1624532.html

7. La ligue du LOL

Léa Lejeune a subi du cyber-harcèlement répété qui démarrait, à chaque fois, par des tweets ou messages d'un membre de la Ligue du LOL. Elle raconte les raids incessants, leur impact sur sa carrière et son engagement pour la défense des femmes journalistes. Nous ne nous sommes pas « senties harcelées », nous l'avons été. Depuis deux jours, cinq d'entre eux m'ont présenté des excuses personnellement par messages privés. C'est soit l'aveu de leur fait d'arme, soit la culpabilité d'avoir laissé les autres faire sans rien dire. Merci messieurs sincèrement, mais nous avons tout de même morflé.

http://www.slate.fr/story/173364/ligue-du-lol-temoignage-journaliste-harcelement-raids

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**.