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 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 Microsoft IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une exécution de code à distance et une usurpation d'identité.	13/02/2019	CVE-2019-0676	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les versions concernées sont les suivantes : Mozilla Firefox de versions antérieures à 65.0.1	13/02/2019	CVE-2019-5785	65.0.1 Télécharger	Mettre à jour le navigateur	10.0

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	13/02/2019	CVE-2019-0664	_	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans le noyau Linux de RedHat	Une vulnérabilité a été découverte dans le noyau Linux de RedHat Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : Red Hat Enterprise Linux Server 6 x86_64 Red Hat Enterprise Linux Server 6 i386 Red Hat Enterprise Linux Workstation 6 x86_64 Red Hat Enterprise Linux Workstation 6 i386	26/02/2019	CVE-2018-10902	5.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2019:0415	10.0

Vulnérabilité dans Google Chrome OS	Google vient de publier une mise à jour de sécurité qui permet de corriger des vulnérabilités au niveau de son système d'exploitation Chrome OS. L'exploitation de ces vulnérabilités peut permettre à un attaquant de causer des problèmes non spécifiés par l'éditeur. Les systèmes infectés sont les suivants : Toutes les versions de chrome OS antérieures à 72.0.3626.117	22/02/2019	–	72.0.3626.117 Contacter	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/02/stable-channel-update-for-chromeos_20.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. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : SUSE Enterprise Storage 4 SUSE CaaS Platform ALL SUSE CaaS Platform 3.0	25/02/2019	CVE-2019-3460	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20190470-1/	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Drupal	Une vulnérabilité critique a été corrigée dans Drupal. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code arbitraire à distance. Les versions affectées sont les suivantes Drupal versions 8.6.x antérieures à 8.6.10 ;	21/02/2019	CVE-2018-1000888	8.6.10 Télécharger	Mettre à jour le CMS	10.0
Vulnérabilité dans le CMS WordPress	Une vulnérabilité a été corrigée dans WordPress. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code arbitraire à distance et de porter atteinte à l'intégrité des données. Les versions affectées sont les suivantes : WordPress toutes les versions antérieures à 5.1	21/02/2019		5.1 Télécharger	Mettre à jour le CMS	10.0

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Microsoft	Plusieurs vulnérabilités ont été corrigées dans certains produits Microsoft. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une élévation de privilèges, une divulgation d'informations, une exécution de code à distance et un déni de service.	13/02/2019	CVE-2019-0686	-	Mettre à jour le système via Windows Update	10.0
Vulnérabilité dans WinRAR	Une vulnérabilité a été corrigée dans WinRAR. L'exploitation de cette vulnérabilité peut permettre à un attaquant d'exécuter du code arbitraire à distance. Les systèmes affectés sont les suivants : WinRAR 5.70 et version antérieure	21/02/2019	–	5.70 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.win-rar.com/latestnews.html?&L=0	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Acrobat et Reader	Une vulnérabilité a été découverte dans Adobe Acrobat et Reader. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : Acrobat DC Continuous versions 2019.010.20091 et antérieures pour Windows et macOS	22/02/2019	CVE-2019-7815	2019.010.20091 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/acrobat/apsb19-13.html	7.8
Vulnérabilité dans les produits VMware	Une vulnérabilité a été découverte dans les produits VMware. Elle permet à un attaquant de provoquer une exécution de code arbitraire. Les versions vulnérables sont : • VMware Integrated OpenStack with Kubernetes (VIO-K) version 5.x • VMware PKS (PKS) versions 12.x et 1.3.x	18/02/2019	CVE-2019-5736	Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2019-0001.html	6.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits CISCO	De multiples vulnérabilités ont été découvertes dans les produits Cisco. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes infectés sont les suivants : • RV110W Wireless-N VPN Firewall versions antérieures à 1.2.2.1 • RV130W Wireless-N Multifunction VPN Router versions antérieures à 1.0.3.45 • RV215W Wireless-N VPN Router versions antérieures à 1.3.1.1 • Cisco Webex Meetings Desktop App versions antérieures à 33.6.6 sur Windows • Cisco Webex Meetings Desktop App versions 33.9.x antérieures à 33.9.1 sur Windows	28/02/2019	CVE-2019-1674	Contacter CISCO	Veuillez-vous référer au bulletin de sécurité Cisco https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190227-rmi-cmd-ex	5.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Thunderbird	De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les produits affectés sont : Thunderbird versions antérieures à 60.5.1	15/02/2019	CVE-2019- 5785	60.5.1 Télécharger	Effectuez une mise à jour du système	5.6

III. ACTUALITÉS

1. Eliminer les mots de passe

C'est peut-être un pas de plus vers un monde sans mots de passe, du moins sur le Web. Le consortium W3C vient d'annoncer que la spécification Web Authentication (WebAuthn) est désormais un standard officiel du Web. Cette annonce n'est pas vraiment une surprise. En avril 2018, WebAuthn avait déjà été promu « Candidate Recommendation », une étape préliminaire pour devenir un standard officiel dans le cadre du W3C.

https://www.01net.com/actualites/le-web-se-dote-d-un-standard-pour-eliminer-les-mots-de-passe-1645865.html

2. L'authentification forte de Facebook affaiblit la protection des données personnelles

Chez Facebook, on est malin. Quand on implémente des fonctions de sécurité informatique, on en profite pour faire d'une pierre deux coups : protéger les utilisateurs, mais aussi augmenter les interactions entre eux, et donc le business. Le Britannique Jeremy Burge vient ainsi découvrir que le numéro de téléphone que l'on renseigne sur le réseau social pour activer l'authentification forte permet à n'importe qui de retrouver le profil Facebook correspondant. Il suffit pour cela de faire un import du numéro au niveau de l'application mobile.

https://www.01net.com/actualites/l-authentification-forte-de-facebook-affaiblit-la-protection-des-donnees-personnelles-1645280.html

3. Une faille 4G et 5G permet de localiser les abonnés

Ce n'est pas avec la 5G que les « IMSI-catcher », ces boîtiers qui permettent d'espionner les abonnés mobiles aux alentours, vont disparaître. Un groupe de cinq chercheurs vient de révéler une nouvelle attaque baptisée « Torpedo » qui permet de savoir si un abonné est présent ou non dans une cellule 4G ou 5G. Le cas échéant, il sera même possible d'en déduire son IMSI, ce fameux identifiant unique utilisé par les opérateurs télécoms. Les chercheurs ont testé leur attaque sur de vrais réseaux.

https://www.01net.com/actualites/une-faille-dans-les-protocoles-4g-et-5g-permet-de-localiser-les-abonnes-1641229.html

4. Cinq questions pour comprendre l'attaque inédite sur internet

Tout part en fait de l'Icann, une autorité de régulation de l'Internet qui s'occupe, entre autres, de l'administration des noms de domaine de premier niveau et de la coordination des acteurs techniques. Dans un communiqué, cette organisation mentionne des attaques sur le système DNS (Domain Name System) qui permet de traduire un nom de domaine en adresse IP.

https://www.01net.com/actualites/cinq-questions-pour-comprendre-l-attaque-inedite-sur-internet-1640558.html

5. Les hackers de Vladimir Poutine mettent moins de 20 minutes pour infester un réseau

Quels sont les états qui disposent des hackers les plus rapides ? Le dernier rapport annuel de la société Crowdstrike donne un premier élément de réponse avec la mesure du « breakout time », c'est-à-dire le temps entre l'infection initiale (le « patient zéro ») et le premier mouvement latéral dans le réseau ciblé. Autrement dit, c'est le temps que mettent les hackers pour commencer à se répandre dans l'infrastructure de la victime.

https://www.01net.com/actualites/les-hackers-de-vladimir-poutine-mettent-moins-de-20-minutes-pour-infester-un-reseau-1636733.html

6. Un lien piégé pour prendre le contrôle de n'importe quel compte Facebook

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/un-lien-piege-suffisait-pour-prendre-le-controle-de-n-importe-quel-compte-facebook-1635429.html

7. Comment les ports thunderbolt permettent de pirater Windows et Linux

Si vous avez un port Thunderbolt sur votre ordinateur, vous avez peut-être un problème. Un groupe de chercheurs vient de publier une étude qui montre que ces interfaces, de plus en plus populaires, peuvent donner accès à la mémoire vive de l'ordinateur. Baptisées « Thunderclap », ces vulnérabilités « permettent à un attaquant disposant d'un accès physique à un port Thunderbolt de compromettre une machine ciblée en l'espace de quelques secondes, d'exécuter du code arbitraire au plus haut niveau de privilège et, potentiellement, d'accéder à des mots de passe, des identifiants bancaires, des clés de chiffrement, des fichiers confidentiels, des données de navigation et autres données ». Tous les systèmes sont impactés, dont Windows, macOS, Linux et FreeBSD. Bref, c'est du lourd.

https://www.01net.com/actualites/comment-les-ports-thunderbolt-permettent-de-pirater-windows-macos-et-linux-1641822.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**.