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 Juin 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	Une vulnérabilité a été découverte dans Google Chrome. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont: Google Chrome versions antérieures à 75.0.3770.90 sur Windows, Mac et Linux.	14/06/2019	CVE-2019-5842	75.0.3770.90 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Mozilla Firefox	Une vulnérabilité a été découverte dans Mozilla Firefox. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : Firefox versions antérieures à 67.0.3	19/06/2019	CVE-2019-11707	67.0.3 Télécharger	Mettre à jour le navigateur	10.0

Vulnérabilité dans Microsoft Internet Explorer	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et une exécution de code à distance. Les systèmes infectés sont les suivants : • Internet Explorer 11 • Internet Explorer 10 • Internet Explorer 9	12/06/2019	CVE-2019-1038	11.706.17134.0	Mettre à jour via Windows Update	9.0
Vulnérabilité dans Microsoft EDGE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une exécution de code à distance et un contournement des fonctionnalités de sécurité.	12/06/2019	CVE-2019-1081	-	Mettre à jour via Windows Update	8.5

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux d'Ubuntu	Une vulnérabilité a été découverte dans le noyau Linux d'Ubuntu. Elle permet à un attaquant de provoquer une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.	25/06/2019	CVE-2019-12817	19.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4031-1/	10.0
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer un contournement des fonctionnalités de sécurité, une élévation de privilèges, une atteinte à la confidentialité des données, une exécution de code à distance et un déni de service.	12/06/2019	CVE-2019-1049	10	Mettre à jour le système via Windows Update	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, un déni de service à distance et un déni de service.	18/06/2019	CVE-2019-9213	8	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2019:1479	10.0

Vulnérabilité dans Google Chrome OS	De multiples vulnérabilités ont été découvertes dans Google Chrome OS. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : Google Chrome OS versions antérieures à 75.0.3770.102 (Platform version: 12105.75.0)	27/06/2019	CVE-2019-11091	75.0.3770.102 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2019/06/stable-channel-update-for-chrome-os-m75.html	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 déni de service à distance une élévation de privilèges, et un autre problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • SUSE Linux Enterprise Live Patching 12-SP3 • SUSE Linux Enterprise Live Patching 12-SP4 • SUSE Linux Enterprise Server 12-LTSS • SUSE Linux Enterprise Server 12-SP1-LTSS • SUSE Linux Enterprise Server 12-SP2-LTSS • SUSE Linux Enterprise Server for SAP 12-SP1 • SUSE Linux Enterprise Server for SAP 12-SP2 • SUSE Linux Enterprise Module for Public Cloud 1	24/06/2019	CVE-2019-11884	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20191692-1/	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le CMS Joomla	De multiples vulnérabilités ont été découvertes dans Joomla! Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité, une atteinte à l'intégrité des données et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Joomla! versions antérieures à 3.9.8	12/06/2019	CVE-2019-12766	3.9.8 Télécharger	Mettre à jour le CMS	8.1

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Excel Power Query	**Bilan de vulnérabilité** : Une vulnérabilité de type zero-day a été découverte dans Microsoft Excel Power Query. Un attaquant pourrait exploiter cette faille afin d'intégrer du contenu malveillant dans une source de données distincte, puis charger le contenu dans un fichier Excel à son ouverture. Le code malveillant pourrait être utilisé pour exécuter des logiciels malveillants susceptibles de compromettre la machine de l'utilisateur, de contourner la politique de sécurité et de porter atteinte à la confidentialité des données. **Solution** : Veuillez-vous référer à l'avis de sécurité Microsoft 4053440 ms qui fournit des conseils pour garantir la sécurité de ces applications Microsoft Office lors du traitement des données de type DDE (Dynamic Data Exchange). https://docs.microsoft.com/en-us/security-updates/securityadvisories/2017/4053440					
Vulnérabilité dans Tenable Nessus	Une vulnérabilité a été découverte dans Tenable Nessus. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Nessus versions antérieures à 8.5.0	26/06/2019	-	8.5.0 Télécharger	Veuillez-vous référer au guide suivant https://www.tenable.com/security/tns-2019-04	5.1

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 une atteinte à la confidentialité des données, une exécution de code à distance, une usurpation d'identité et un déni de service. Les produits affectés sont les suivants : • Azure DevOps Server 2019 • ChakraCore • Microsoft Lync Server 2010 • Microsoft Lync Server 2013	12/06/2019	CVE-2019-1052	-	Effectuez une mise à jour via Windows Update	10.0
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une exécution de code à distance et une usurpation d'identité.	12/06/2019	CVE-2019-1036	2019	Mettre à jour le système via Windows Update	7.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans VideoLAN VLC	De multiples vulnérabilités ont été découvertes dans VideoLAN VLC. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et un déni de service. Les versions affectées sont les suivantes: VLC media player versions 3.0.6 et antérieures	21/06/2019	CVE-2019-5439	3.0.7.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.videolan.org/security/sa1901.html	10.0
Vulnérabilité dans Apple AirPort	Plusieurs vulnérabilités ont été corrigées dans Apple AirPort. L'exploitation de ces vulnérabilités peut permettre à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement des politiques de sécurité Les versions affectées sont les suivantes : AirPort Express, AirPort Extreme et AirPort Time Capsule base stations compatible 802.11n sans la mise à jour du microgiciel version 7.8.1	21/06/2019	CVE-2019-12436	Contacter Apple	Veuillez-vous référer au Bulletin de sécurité https://support.apple.com/en-us/HT210091	7.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le DNS de BIND	Une vulnérabilité a été corrigée dans le DNS de BIND. Un attaquant pourrait exploiter cette vulnérabilité afin de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • BIND versions 9.11.0 à 9.11.7, 9.12.0 à 9.12.4-P1 et 9.14.0 à 9.14.2 • BIND toutes versions 9.13 et 9.15 • BIND Supported Preview Edition versions 9.11.3-S1 à 9.11.7-S1	20/06/2019	CVE-2019-6471	9.15.1 Télécharger	Veuillez-vous référer au bulletin de sécurité https://kb.isc.org/docs/cve-2019-6471	3.2
Vulnérabilité dans les produits Cisco	Cisco annonce la correction de plusieurs vulnérabilités dans certains de ses produits. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance, provoquer un déni de service ou accéder à des données confidentielles.	21/06/2019	CVE-2019-1878	-	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190619-cms-codex	4.5

III. ACTUALITÉS

1. Comment remplacer Windows 7 ?

Beaucoup d'entre vous sont des utilisateurs de Windows 7. Je le comprends. Windows 7 fonctionne bien. Toutefois, l'horloge tourne : dans moins d'un an, le support gratuit de Windows 7 prend fin. Le jour venu, vous aurez le choix : soit vous l'exécutez sans être sûr d'obtenir les correctifs de sécurité essentiels (ce serait vraiment stupide), soit vous payez les mises à jour de sécurité étendues de Windows 7 (ESU) par appareil, le prix augmentant chaque année. Nous ne savons pas quel sera le coût, mais nous pouvons supposer que ce ne sera pas bon marché. Sinon, vous pouvez aussi migrer vers Windows 10. Pour l'instant, vous pouvez encore faire la mise à jour vers Windows 10 gratuitement à partir de Windows 7.

https://www.zdnet.fr/actualites/comment-remplacer-windows-7-par-linux-mint-39886865.htm#xtor=RSS-1

2. Une dizaine d'opérateurs télécoms mondiaux hackés

Des pirates informatiques ont pénétré dans les systèmes de plus d'une dizaine d'opérateurs de télécommunications dans le monde, récoltant de grandes quantités d'informations sur leurs clients révèle Cybereason. L'éditeur de cybersécurité, fondé par d'anciens spécialistes renseignement militaire israélien mais basé à Boston, estime que les hackers travaillent pour le gouvernement chinois. Les outils et techniques utilisés tout au long de ces attaques sont en effet compatibles avec ceux dont se sert le groupe de hackers APT10, censé agir pour le compte du ministère chinois de la Sécurité de l'État.

https://www.informatiquenews.fr/une-dizaine-doperateurs-telecoms-mondiaux-ainsi-que-des-geants-de-lit-hackes-62578

3. Le Botnet Scranos de retour

En avril dernier, Bitdefender a révélé l'émergence d'un botnet appelé Scranos. Originaire de Chine, celui-ci s'est propagé en Europe et aux États-Unis, piégeant des appareils Windows et Android dans le cadre de fraudes publicitaires et de manipulations des réseaux sociaux. Le rapport initial de Bitdefender pointait du doigt les exploitants de Scranos et dénonçait leur utilisation illégale de certificats Authenticode, entre autres. Après que Bitdefender ait contacté Digicert pour lui signaler le certificat utilisé pour signer le pilote du rootkit à des fins malveillantes, les exploitants de Scranos ont perdu le principal mécanisme leur permettant d'assurer leur durabilité et leur camouflage. Lorsque le rapport Scranos a été publié, les attaquants ont vu leur infrastructure de commande et contrôle épinglée pour activité malveillante et démantelée.

https://www.undernews.fr/malwares-virus-antivirus/botnet-scranos-le-retour.html

4. Les activités d'harponnage menées par le groupe apt33

FireEye a identifié des activités de 'spearphishing' (harponnage) conduites par le groupe de menaces iranien APT33 en parallèle avec un climat de tension accru dans la région du Golfe et avec les Etats Unis. La campagne de 'spearphishing' a ciblé à la fois les secteurs privé et public aux Etats Unis. Cette activité est compatible avec la collecte de renseignements, et il est probable que le régime iranien utilise aussi du cyber espionnage pour réduire ses incertitudes entourant le conflit. A noter qu'APT33 a dans le passé effectué des attaques destructrices s'ajoutant à la collecte de renseignements.

https://www.undernews.fr/hacking-hacktivisme/fireeye-a-identifie-des-activites-de-spearphishing-harponnage-conduites-par-le-groupe-de-menaces-iranien-apt33.html

5. Le portail pédopornographique Blackhealth définitivement fermé

La Police provinciale de l'Ontario vient de faire fermer, ce 12 juin 2019, une importante boutique de black market spécialisée dans l'achat et la vente de documents pédopornographiques. Selon les autorités, l'enquête – baptisée Project Greenwell / project Blackheath – a débuté en 2012. Elle visait un fournisseur de millions d'images et de vidéos pédophiles. La police décrit ce portail comme un « une grande surface de pornographie enfantine «. Plus 59 995 utilisateurs dans au moins 116 pays différents.

https://www.zataz.com/black-market-blackheath-pedopornographie/

6. La nouvelle variante de Dridex

Researchers have spotted a variant of the Dridex banking trojan with new obfuscation capabilities that help it skirt anti-virus detection. While Dridex has been around since 2011, researchers told Threatpost Friday that they recently spotted phishing emails distributing a never-before-seen variant of the malware. This variant uses file signatures that are difficult for anti-virus software to sniff out – allowing the malware to evade detection when on infected systems.

https://threatpost.com/new-dridex-variant-slips-by-anti-virus-detection/146134/

7. Un adolescent de 14 ans crée un malware qui détruit de nombreux objets connectés

Le monde des objets connectés a peut-être évité de justesse une nouvelle catastrophe. Il y a quelques jours, un hacker a lancé Silexbot, un malware qui tente de se connecter à des objets connectés sur Internet via le protocole Telnet. A l'instar du ver Mirai, il utilise pour cela une liste d'identifiants usuels, tel que root/password. Une technique ultra-classique.

https://www.01net.com/actualites/un-adolescent-a-cree-un-malware-qui-a-detruit-des-milliers-d-objets-connectes-1721716.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. Microsoft annonce la fin du support de toutes les versions de Windows 7 à partir du 14 janvier 2020. Après cette date les systèmes fonctionnant sous Microsoft Windows 7 ne recevront plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
4. 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.
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**.