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 d'Octobre 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. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont : Google Chrome versions antérieures à 77.0.3865.120 pour Windows, Mac et Linux.	11/10/2019	CVE-2019-13697	77.0.3865.120 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Microsoft IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une exécution de code à distance et une usurpation d'identité. Les systèmes concernés sont les suivants : • Internet Explorer 10 • Internet Explorer 11 • Internet Explorer 9	09/11/2019	CVE-2019-1371	10	Mettre à jour le système via Windows Update	10.0

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 une usurpation d'identité.	09/10/2019	CVE-2019-1366	-	Mettre à jour le système via Windows Update	9.0

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. 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. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Server for SAP 12-SP2 • SUSE Linux Enterprise Server for SAP 12-SP1 • SUSE Linux Enterprise Server 12-SP2-LTSS	09/10/2019	CVE-2019-14835	-	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20192572-1/	10.0

	• SUSE Linux Enterprise Server 12-SP1-LTSS • SUSE Linux Enterprise Server for SAP 12-SP3 • SUSE Linux Enterprise Server 12-SP3-LTSS • SUSE Linux Enterprise Server for SAP 12-SP2 • SUSE Linux Enterprise Server 12-SP2-LTSS • SUSE Linux Enterprise Module for Live Patching 15-SP1 • SUSE Linux Enterprise Module for Live Patching 15 • SUSE Linux Enterprise Live Patching 12-SP4					
Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau linux d'Ubuntu. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Ubuntu 19.04 • Ubuntu 18.04 LTS	07/10/2019	CVE-2019-15926	19.4 Télécharger	Veuillez-vous mettre à jour votre système	10.0

Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. La version affectée est la suivante : Google Android toutes versions n'intégrant pas le correctif de sécurité du 07 octobre 2019	07/10/2019	CVE-2019-10566	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/pixel/2019-10-01	10.0
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, un contournement de la fonctionnalité de sécurité, une usurpation d'identité, une exécution de code à distance, une élévation de privilèges et un déni de service.	09/10/2019	CVE-2019-1378	10	Mettre à jour le système via Windows Update	10.0

II.3 AUTRES

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 et une usurpation d'identité. Les systèmes infectés sont les suivants : • Azure App Service on Azure Stack • ChakraCore • Microsoft Dynamics 365 (on-premises) version 9.0 • Open Enclave SDK • SQL Server Management Studio 18.3 • SQL Server Management Studio 18.3.1	09/10/2019	CVE-2019-1376	-	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 élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	09/10/2019	CVE-2019-1331	2019	Mettre à jour le système via Windows Update	8.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Zimbra	De multiples vulnérabilités ont été découvertes dans Zimbra. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les systèmes infectés sont les suivants : • Zimbra 8.8.15 “James Prescott Joule” versions antérieures au Patch 2 • Zimbra 8.8.12 “Isaac Newton” versions antérieures au Patch 6 • Zimbra 8.7.11 versions antérieures au Patch 14	01/10/2019	CVE-2019-12625	8.8.15 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://blog.zimbra.com/2019/09/new-zimbra-patches-8-8-15-patch-2-and-8-8-12-patch-6-and-8-7-11-patch-14/	6.8
Vulnérabilité dans les produits Juniper	De multiples vulnérabilités ont été découvertes dans les produits Juniper. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.	10/10/2019	CVE-2019-0067	Contacter Juniper	Veuillez-vous référer au bulletin de sécurité https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10966&cat=SIRT_1&actp=LIST	6.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Les produits Intel	De multiples vulnérabilités ont été découvertes dans les produits Intel. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges. Les produits infectés sont les suivants : • Intel NUC 8 Mainstream Game Kit sans le correctif de sécurité INWHL357 • Intel NUC 8 Mainstream Game Mini Computer sans le correctif de sécurité INWHL357 • Intel NUC Board DE3815TYBE (H26998-500 & later) sans le correctif de sécurité TY0022 • Intel NUC Kit DE3815TYKHE (H27002-500 & later) sans le correctif de sécurité TY0022 • Intel NUC Board DE3815TYBE sans le correctif de sécurité TY0067 • Intel NUC Kit DE3815TYKHE sans le correctif de sécurité TY0067	08/10/2019	CVE-2019-14570	Contacter Intel	Veuillez-vous référer au bulletin de sécurité https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00261.html	4.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• Intel NUC Kit DN2820FYKH sans le correctif de sécurité FY0069 • Intel Smart Connect Technology pour Intel NUC (la désinstallation est recommandée par Intel) • Intel Active System Console for Intel Server Boards and Systems based on Intel 62X Chipset versions antérieures à 8.0 Build 24					
Vulnérabilité dans les solutions VPN VPN Fortinet, Pulse Secure et Palo Alto	De nouveaux exploits ont été publiés ciblant les solutions VPN Fortinet, Pulse Secure et Palo Alto. L'exploitation des vulnérabilités correspondantes permettrait à un attaquant de récupérer des données confidentielles sur le serveur VPN sans devoir s'authentifier. Il est recommandé aux entités disposant de ces technologies de vérifier l'effectivité des mises à jour. Veuillez-vous référer aux bulletins de sécurité afin d'installer les dernières mises à jour : Palo Alto: ➢ https://securityadvisories.paloaltonetworks.com/(X(1)S(klphdezgerjfyhnvfqkwlgqu))/Home/Detail/158?AspxAutoDetectCookieSupport=1 FortiGuard: ➢ https://fortiguard.com/psirt/FG-IR-18-384 ➢ https://fortiguard.com/psirt/FG-IR-18-388 ➢ https://fortiguard.com/psirt/FG-IR-18-389 Pulse Secure: ➢ https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101					

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	systems infectés : ➢ Palo Alto PAN-OS 7.1.18 et version antérieure, PAN-OS 8.0.11-h1 et version antérieure, PANOS 8.1.2 et version antérieure. ➢ FortiOS 6.2.X version antérieure 6.2.0 ➢ FortiOS 6.0.X version antérieure 6.0.5 ➢ FortiOS 5.6.X version antérieure 5.6.8 ➢ FortiOS 5.4.X version antérieure 5.4.13 ➢ Pulse Connect Secure 9.0RX version antérieure à Pulse Connect Secure 9.0R3.4 & 9.0R4 ➢ Pulse Connect Secure 8.3RX version antérieure à Pulse Connect Secure 8.3R7.1 ➢ Pulse Connect Secure 8.2RX version antérieure à Pulse Connect Secure 8.2R12.1 ➢ Pulse Connect Secure 8.1RX version antérieure à Pulse Connect Secure 8.1R15.1 ➢ Pulse Policy Secure 9.0RX version antérieure à Pulse Policy Secure 9.0R3.2 & 9.0R4 ➢ Pulse Policy Secure 5.4RX version antérieure à Pulse Policy Secure 5.4R7.1 ➢ Pulse Policy Secure 5.3RX version antérieure à Pulse Policy Secure 5.3R12.1 ➢ Pulse Policy Secure 5.2RX version antérieure à Pulse Policy Secure 5.2R12.1 ➢ Pulse Policy Secure 5.1RX version antérieure à Pulse Policy Secure 5.1R15.1					

III. ACTUALITÉS

1. 861 Million SIM cards in 29 Countries are Vulnerable to Simjacker Attacks

La vulnérabilité Simjacker révélée le mois dernier, a été exploitée depuis plus de deux ans par des attaquants. Cette vulnérabilité est basée sur la technologie de la carte SIM. La vulnérabilité repose sur la technologie S @ T Browser, qui ne dispose d'aucune authentification activée par défaut. Elle permet aux attaquants d'exécuter toute commande sur la carte SIM sans le consentement de l'utilisateur.

https://www.itsecuritynews.info/861-million-sim-cards-in-29-countries-are-vulnerable-to-simjacker-attacks/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ItSecurityNewsAggregated+%28IT+Security+News%29

2. Le quotidien des agents de renseignement

Se montrer sans rien dévoiler. Se raconter sans trahir de secret. C'est l'exercice acrobatique auquel des agents de la Direction générale de la sécurité intérieure (DGSI) et de la Direction générale de la sécurité extérieure (DGSE), les deux principaux services de renseignement français, ont accepté de se livrer pour Le Parisien-Aujourd'hui en France

http://www.leparisien.fr/faits-divers/que-font-vraiment-nos-espions-des-agents-du-renseignement-racontent-leur-metier-13-10-2019-8171799.php#xtor=RSS-1481423633

3. Sophisticated Spy Kit Targets Russians with Rare GSM Plugin

Une plate-forme de cyberespionnage sophistiquée appelée Attor a été révélée. Selon les chercheurs d'ESET, Attor, qui a survolé le radar depuis au moins 2013, présente également une architecture modulaire complexe et des communications réseau élaborées utilisant Tor, ce qui en fait une menace extrêmement évoluée.

https://threatpost.com/sophisticated-spy-kit-russians-gsm-plugin/149095/

4. Chrome va bientôt bloquer tous les contenus non chiffrés des sites web HTTPS

Google, on le sait, milite pour une généralisation du protocole de chiffrement HTTPS, qui apporte une bien meilleure sécurité pour les internautes que le simple protocole HTTP. Il n'est donc pas étonnant que le géant informatique décide de bloquer prochainement tous les contenus non chiffrés dans les sites HTTPS.

https://www.01net.com/actualites/chrome-va-bientot-bloquer-tous-les-contenus-non-chiffres-des-sites-web-https-1780604.html

5. L’usage des applis espionnes augmente de façon inquiétante

Espionner un proche au travers de son smartphone est un phénomène qui prend de l’ampleur. Parmi les utilisateurs Android de Kaspersky, plus de 37 000 ont fait l’expérience désagréable de détecter un mouchard sur leur terminal mobile entre janvier et août 2019. Ce qui représente une augmentation de 35 % par rapport à 2018. Ces utilisateurs espionnés vivent principalement en Russie, en Inde, au Brésil et aux Etats-Unis. La France n’arrive qu’en 9e position, et c’est tant mieux

https://www.01net.com/actualites/l-usage-des-applis-espionnes-augmente-de-facon-inquietante-1779927.html

6. Une faille irréparable du standard PDF permet le vol de tous les contenus, même chiffrés

Le PDF est un format de document extrêmement populaire, y compris pour manipuler des données sensibles. En effet, ce standard propose un chiffrement natif fort pratique, censé rendre les données inviolables. Pour l’activer, il suffit généralement de définir un mot de passe au niveau du logiciel PDF. Mais ce chiffrement est loin d’être inviolable, comme vient de le montrer un groupe de chercheurs des universités Ruhr-Bochum et Munster. Ces experts ont trouvé deux attaques baptisées « PDFex », permettant de faire fuiter les informations confidentielles d’un fichier PDF chiffré.

https://www.01net.com/actualites/une-faille-irreparable-du-standard-pdf-permet-le-vol-de-tous-les-contenus-meme-chiffres-1778350.html

7. Les câbles Lighting piégés sont désormais produits en masse

En février dernier, le hacker Mike Grover avait présenté un dispositif fort étrange. Baptisé « O.MG Cable », il ressemble à un câble Lighting, ce qu’il est d’ailleurs. Mais ce n’est pas tout. Il embarque également un tout petit module Wi-Fi grâce auquel une tierce personne peut envoyer des commandes HID (Human Interface Device) à l’ordinateur auquel il est connecté, simplement au travers d'une application mobile. Ces commandes permettent de simuler un clavier ou une souris et, par conséquent, de prendre le contrôle de l’ordinateur.

https://www.01net.com/actualites/les-cables-lighting-pieges-sont-desormais-produits-en-masse-1778047.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**.