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 Septembre 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 3
II. VULNÉRABILITÉS PUBLIÉES 4
II.1 NAVIGATEURS 4
Vulnérabilité dans Google Chrome 4
Vulnérabilité dans Mozilla Firefox 4
II.2 SYSTÈMES D'EXPLOITATION 5
Vulnérabilité dans le noyau Linux de SUSE 5
Vulnérabilité dans le noyau Linux de Debian 5
Vulnérabilité dans le noyau Linux d'Ubuntu 6
II.1 CMS 7
Vulnérabilité dans Moodle 7
Vulnérabilité dans Joomla 7
II.2 AUTRES 8
Vulnérabilité dans les produits Cisco 8
Vulnérabilité dans les produits VMware 8
Vulnérabilité dans Libreoffice 9
Vulnérabilité dans dlink -- dns-320_firmware 9
Vulnérabilité dans curl 9
Vulnérabilité dans Microsoft IE et Defender 10
III. ACTUALITÉS 11
IV. NOTES IMPORTANTES 13

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 : Chrome, versions antérieures à 77.0.3865.90 sur Windows, Mac et Linux	19/09/2019	CVE-2019-13688	77.0.3865.90 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 un contournement de la politique de sécurité. Les systèmes affectés sont : Firefox versions antérieures à 69.0.1	19/09/2019	CVE-2019-11754	69.0.1 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 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, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes infectés sont les suivants : • SUSE Linux Enterprise Module for Realtime 15-SP1 • SUSE Linux Enterprise Module for Open Buildservice Development Tools 15-SP1 • SUSE Linux Enterprise Real Time Extension 12-SP4	24/09/2019	CVE-2019-14284	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2019/suse-su-20192450-1/20192262-1/	10.0
Vulnérabilité dans le noyau Linux de Debian	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges. Les versions affectées sont les suivantes : • Debian stretch versions antérieures à 4.9.189-3+deb9u1 • Debian buster versions antérieures à 4.19.67-2+deb10u1	26/09/2019	CVE-2019-15902	10.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.debian.org/security/2019/dsa-4531	10.0

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 à distance, 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 • Ubuntu 16.04 LTS • Ubuntu 14.04 ESM • Ubuntu 12.04 ESM	18/09/2019	CVE-2019-15031	19.4 Télécharger	Veuillez-vous mettre à jour votre système	10.0
	Une faille de débordement de mémoire tampon a été découverte dans le Kernel Linux, dans la manière dont la fonctionnalité de transformation de tampon de file virtuelles en IOVs, Un utilisateur sans privilèges capable de transmettre des descripteurs de longueur non valide à l'hôte lorsque la migration est en cours pourrait utiliser cette vulnérabilité pour augmenter ses privilèges sur l'hôte. Les verrsions affectées sont les suivantes : Kernel Linux 2.6.34 à 5.2.x	17/09/2019	CVE-2019-14835	19.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4135-2/	7.2

II.1 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, un contournement de la politique de sécurité et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Moodle versions antérieures à 3.5.8 • Moodle versions 3.6.x antérieures à 3.6.6 • Moodle versions 3.7.x antérieures à 3.7.2	16/09/2019	CVE-2019-14831	3.7.2 Télécharger	Mettre à jour le CMS	8.1
Vulnérabilité dans Joomla	Une vulnérabilité a été découverte dans Joomla. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). La version affectée est la suivante : Joomla versions antérieures à 3.9.12	25/09/2019	CVE-2019-16725	3.9.12 Télécharger	Mettre à jour le CMS	8.1

II.2 AUTRES

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, un déni de service à distance et un contournement de la politique de sécurité.	26/09/2019	CVE-2019-12658	-	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925	8.8
Vulnérabilité dans les produits VMware	Une vulnérabilité a été découverte dans les produits VMware. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions vulnérables sont : • VMware Cloud Foundation • VMware Harbor Container Registry for PCF versions 1.8.x antérieures à 1.8.3 • VMware Harbor Container Registry for PCF versions 1.7.x antérieures à 1.7.6	25/09/2019	CVE-2019-16097	Contacter VMware	Veuillez-vous référer au bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2019-0015.html	6.2

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 un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • LibreOffice versions antérieures à 6.2.6 • LibreOffice versions 6.3.x antérieures à 6.3.1	27/09/2019	CVE-2019-9853	6.3.1 Télécharger	Veuillez-vous référer au bulletin de sécurité https://www.libreoffice.org/about-us/security/advisories/cve-2019-9853/	3.1
Vulnérabilité dans dlink-- dns-320_firmware	Le script login_mgr.cgi de D-Link DNS-320 à 2.05.B10 est vulnérable à l'injection de commandes à distance.	16/09/2019	CVE-2019-16057	-	Veuillez-vous référer au guide suivant : https://blog.cystack.net/d-link-dns-320-rce/	10.0
Vulnérabilité dans curl	Une vulnérabilité de type dépassement de mémoire tampon dans le gestionnaire de protocole TFTP a été découverte dans cURL de version 7.19.4 à 7.65.3.	16/09/2019	CVE-2019-5482	7.66.0 Télécharger	Mettre à jour en version 7.66.0 ou ultérieure	7.5
	Une vulnérabilité de type double-free a été découverte dans le code FTP-kerberos dans cURL de version 7.52.0 à 7.65.3.	16/09/2019	CVE-2019-5481			7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft IE et Defender	De multiples vulnérabilités ont été découvertes dans Microsoft IE et Defender. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service. Les systèmes affectés sont les suivants : • Internet Explorer 9 sur toutes les versions de Windows supportées • Internet Explorer 10 sur toutes les versions de Windows supportées • Internet Explorer 11 sur toutes les versions de Windows supportées • Microsoft Defender sur toutes les versions de Windows supportées	24/09/2019	CVE-2019-1367	-	Mettre à jour le système via Windows Update	6.3

III. ACTUALITÉS

1. La compagnie AirBus ciblée par des cyberattaques

D'après plusieurs sources, les piratages en question semblent tous avoir été pilotés depuis la Chine. Au bilan des actes de cyber-espionnage industriel, ce sont quatre attaques majeures ayant visé des sous-traitants de Airbus au cours des douze derniers mois qui ont été recensées. Plus d'une demi-douzaine de sources proches du dossier, s'exprimant sous couvert d'anonymat ont permis de dessiner les contours et objectifs de cette série d'offensives. La Chine est d'ores-et-déjà pointée du doigt et des soupçons pèsent…

https://www.undernews.fr/hacking-hacktivisme/cyber-espionnage-des-cyberattaques-ciblent-airbus.html

2. Le groupe Lazarus prend pour cible des guichets automatiques

Ils auraient développé un logiciel malveillant en mesure de dérober des données dans les guichets automatiques du pays. Ce programme surnommé ATMDtrack vise les distributeurs de billets depuis l'été dernier. Il est en mesure de lire et stocker les données associées aux cartes insérées dans les machines infectées.

https://www.presse-citron.net/apres-wannacry-le-groupe-de-hackers-nord-coreens-lazarus-prend-pour-cible-les-guichets-automatiques/

3. Un ransomware perturbe la fabrication d'armes

L'un des plus importants fabriquant de véhicules militaires au monde se retrouve confronté à un ransomware. L'outil pirate a pris en otage le réseau de la société. Il provoque des perturbations importantes dans des usines brésiliennes, américaines et mexicaines.

https://www.zataz.com/rheinmetall-un-ransomware-perturbe-la-production-dun-important-fabriquant-darmes/

4. Les faux bloqueurs de pub

Faux bloqueurs de publicité ! Selon une étude menée par la société Adguard, deux bloqueurs de publicités accessibles pour Chrome sont des faux widgets. Mission, effectuer des fraudes publicitaires à grande échelle en utilisant le nom de bloqueurs de publicités légitimes. Ce n'est d'ailleurs pas une nouveauté. L'année derniére déjà, cinq faux avaient été repérés : Webutation (30 000 télédchargements), HD for YouTube (400 000), Adblock Pro (2 millions), uBlock Plus (8 millions d'utilisateurs) ou encore AdRemover (10 millions).

https://www.zataz.com/faux-bloqueurs-pubs/

5. Des pentesters arrêtés après une intrusion physique

Des pentesters arrêtés pour s'être infiltrés dans un palais de justice. Il était en mission pour tester les vulnérabilités du bâtiment. Leur contrat de travail ne stipulait pas les actions physiques possibles dans ce genre de métier. Ils ont déclaré aux forces de l'ordre tester les vulnérabilités physiques de l'établissement (alarmes, …). Équipés de nombreux outils de cambriolage, ils devaient évaluer le temps de réponse des forces de l'ordre

https://www.zataz.com/pentesters-arretes-intrusion-physique/

6. Le cyberbunker démantelé

C'est un joli coup de filet. Fin de semaine dernière, plusieurs centaines d'agents de police, dont l'unité d'intervention spéciale GSG9, ont démantelé un hébergeur de services illégaux du Darknet. Il était installé dans un ancien bunker de l'Otan, près de Traben-Trarbach, une bucolique petite ville située en Rhénanie-Palatinat. Cette casemate a été rachetée en 2013 par un Néerlandais de 59 ans pour le transformer en un datacenter dit « bullet-proof », c'est-à-dire à l'abri des enquêtes de police. Dans le milieu du Darknet, cet hébergeur était connu sous le nom de « Cyberbunker ».

https://www.01net.com/actualites/la-police-allemande-demantele-le-cyberbunker-un-important-datacenter-illegal-1777385.html

7. Un jailbreak impossible à patcher

Les bidouilleurs peuvent à nouveau se frotter les mains. Le hacker « axi0mX » vient de publier un jailbreak baptisé « checkm8 », permettant de cibler tous les appareils iOS, allant de la puce A5 à la puce A11. Cela concerne donc les smartphones de l'iPhone 4s à l'iPhone X, et les tablettes de l'iPad 2 à l'iPad de 6e génération. Au final, plusieurs *« centaines de millions d'appareils »* seraient donc vulnérables selon axi0mX.

https://www.01net.com/actualites/un-jailbreak-impossible-a-patcher-cible-tous-les-iphone-et-ipad-sauf-les-derniers-1777316.html

8. Attaque Simjacker : environ 10 % des cartes SIM sont vulnérables

La faille qui permet de géolocaliser les utilisateurs par l'envoi d'un SMS invisible n'est, heureusement, pas si fréquente que cela. Mais concerne tout de même plusieurs centaines de millions de terminaux.

https://www.01net.com/actualites/attaque-simjacker-environ-10percent-des-cartes-sim-sont-vulnerables-1777450.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**.