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 Mai 2020

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 versions affectées sont : Google Chrome versions antérieures à 83.0.4103.61	20/05/2020	CVE-2020-6491	83.0.4103.61 Télécharger	Mettre à jour le navigateur	10.0
Vulnérabilité dans Microsoft EDGE	Une vulnérabilité a été découverte dans Microsoft Edge. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions affectées sont les suivantes : Microsoft Edge (Chromium-based) versions antérieures à 83.0.478.37	22/05/2020	CVE-2020-1195	-	Mettre à jour 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 problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire à distance et un déni de service à distance.	25/05/2020	CVE-2020-11609	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20201275-1/	10.0
Vulnérabilité dans le noyau Linux de 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 20.04 LTS • Ubuntu 19.10 • Ubuntu 18.04 LTS	29/05/2020	CVE-2020-12657	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4369-2/	10.0

Vulnérabilité dans le noyau Linux de Red Hat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une élévation de privilèges.	26/05/2020	CVE-2020-11884	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:2289	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 versions affectées sont les suivantes : Google Chrome OS versions antérieures à 83.0.4103.77 (Platform version: 13020.55.0 or 13020.55.1)	28/05/2020		OS 83	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/05/stable-channel-update-chrome-os.html	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Drupal	De multiples vulnérabilités ont été découvertes dans Drupal. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et une injection de code à distance (XSS). Les versions affectées sont : • Drupal core versions antérieures à 7.70 • Drupal core versions 8.x antérieures à antérieures à 8.7.14 • Drupal core versions 8.8.x antérieures à 8.8.6	22/05/2020	CVE-2020-11023	8.8.6 Télécharger	Mettre à jour le CMS	4.5
Vulnérabilité dans WordPress	Plusieurs vulnérabilités ont été corrigées dans le plugin PageLayer du CMS WordPress. L'exploitation de ces failles pourrait permettre à un attaquant distant de réussir une élévation de privilèges ou d'exécuter du code arbitraire à distance. Les systèmes affectés sont les suivants : WordPress Plugin PageLayer version antérieure à 1.1.4;	29/05/2020		5.4.1 Télécharger	Mettre à jour le plugin en version 1.1.4 ou ultérieure	3.6

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits VMware	De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer un déni de service et une élévation de privilèges. Les versions concernées sont les suivantes : • VMware Fusion versions 11.x antérieures à sur OS X • VMware VMRC pour Mac versions 11.x sur OS X • VMware Horizon Client pour Mac versions 5.x et antérieures sur OS X • VMware ESXi versions 6.7.x antérieures à ESXi670-202004101-SG • VMware ESXi versions 6.5.x antérieures à ESXi650-202005401-SG • VMware Workstation versions 15.x antérieures à 15.5.2 • VMware Fusion versions 11.x antérieures à 11.5.2 sur OS X	29/05/2020	CVE-2020-3959		Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2020-0011.html	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • GitLab Community Edition (CE) et Enterprise Edition (EE) versions 13.0.x antérieures à 13.0.1 • GitLab Community Edition (CE) et Enterprise Edition (EE) versions 12.10.x antérieures à 12.10.7 • GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 12.9.8	28/05/2020			Veuillez-vous référer au Bulletin de sécurité https://about.gitlab.com/releases/2020/05/27/security-release-13-0-1-released/	10.0
Vulnérabilité dans Wireshark	Une vulnérabilité a été découverte dans Wireshark. Elle permet à un attaquant de provoquer un déni de service à distance. Les systèmes infectés sont les suivants : • Wireshark versions 3.2.x antérieures à 3.2.4 • Wireshark versions 3.0.x antérieures à 3.0.11 • Wireshark versions antérieures à 2.6.17	20/05/2020		3.2.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.wireshark.org/security/wnpa-sec-2020-08.html	7.7

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 atteinte à l'intégrité et à la confidentialité des données. Les versions affectées sont les suivantes : • LibreOffice versions 6.3.x antérieures à 6.3.6 • LibreOffice versions antérieures à 6.4.3	18/05/2020	CVE-2020-12801	6.4.4 Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://www.libreoffice.org/about-us/security/advisories/cve-2020-12801/	8.2
Vulnérabilité dans Docker Desktop	Docker annonce la publication d'une nouvelle mise à jour qui corrige une vulnérabilité critique dans Docker Desktop. L'exploitation de cette faille peut permettre à un attaquant d'exécuter du code arbitraire avec des privilèges SYSTEM. Les produits affectés sont les suivants : • Docker Desktop version antérieure à 2.3.0.2 ;	29/05/2020	CVE-2020-11492	2.3.0.x Télécharger	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://docs.docker.com/docker-for-windows/release-notes/	10.0

II.5 Actualités

1. **Une faille dans un système embarqué permet de prendre le contrôle d'un véhicule à distance**
   Cette vulnérabilité permet d'exploiter à des fins malveillantes les systèmes Linux ARMv7, des systèmes notamment présents dans les véhicules connectés. La faille rend possible la mise en œuvre de vulnérabilités logicielles, d'attaques basées sur le matériel et, selon le blog de Talos Intelligence, permettrait de prendre le contrôle d'un véhicule à distance.
   https://www.undernews.fr/alertes-securite/voitures-connectees-une-faille-dans-un-systeme-embarque-permet-de-prendre-le-controle-dun-vehicule-a-distance.html

2. **Les hackers éthiques totalisent 100 millions de dollars de récompenses sur HackerOne**
   HackerOne, première plateforme mondiale de sécurité collaborative, annonce aujourd'hui que sa communauté de hackers éthiques a totalisé 100 millions de dollars de primes aux bugs sur sa plateforme. Une prime – ou bug bounty – est une récompense financière donnée à un hacker qui trouve une faille de sécurité et la signale à une organisation afin qu'elle puisse être comblée.
   https://www.undernews.fr/hacking-hacktivisme/les-hackers-ethiques-totalisent-100-millions-de-dollars-de-recompenses-sur-hackerone.html

3. **Zeppelin, le ransomware qui fait des promos**
   Zeppelin se veut discret, sans double chantage. Il évolue aussi sous le nom de Buran. Cet outil pirate est apparu dans plusieurs commerces pirates en avril et mai 2019. Comme ses « grands frères » , Zeppelin, baptisé aussi Zappelin, est un Ransomware-as-a-Service (RaaS). Comprenez qu'il est loué par ses auteurs à d'autres pirates. « nous voulons être présents sur le marché sous toutes les formes qui nous sont avantageuses. » expliquaient les auteurs en mai 2019.
   https://www.zataz.com/zeppelin-le-ransomware-qui-fait-des-promos/

4. **Google propose le programme de protection avancée aux appareils Nest**
   Google a annoncé aujourd'hui qu'il apportait son programme de protection avancée à Nest pour apporter le plus haut niveau de protection à votre domicile.Le programme de protection avancée de Google s'adresse à des cibles à haut risque telles que les journalistes, les militants, les chefs d'entreprise et les équipes politiques, mais il est aussi accessible à tous.

   https://www.bleepingcomputer.com/news/google/google-brings-the-advanced-protection-program-to-nest-devices/

5. **Une fuite de données de Joomla révèle 2 700 enregistrements d'utilisateurs via des sauvegardes exposées**
   Une fuite dans la base de données Joomla a révélé les informations personnelles, y compris les mots de passe hachés, de 2 700 personnes enregistrées dans le répertoire des ressources Joomla (JRD). Le répertoire de ressources Joomla permet aux utilisateurs de trouver des fournisseurs de services enregistrés pour aider à la gestion de projet, à la conception et au support technique de Joomla. Dans un avis de sécurité publié par Joomla la semaine dernière, il a été révélé que les détails de 2 700 personnes enregistrées sur le service Joomla Resources Directory (JRD) avaient été divulgués.

   https://www.bleepingcomputer.com/news/security/joomla-data-breach-leaks-2-700-user-records-via-exposed-backups/

6. **Les navigateurs Web autorisent toujours les attaques de type drive-by-downloads en 2020**
   Nous sommes en 2020, et de nombreux navigateurs autorisent toujours les téléchargements via des attaques de type drive-by-download à partir de ce qui est censé être des contextes sécurisés tels que les iframes isolés. Pour ceux qui ne connaissent pas le terme, drive-by-download se produit lorsqu'un utilisateur visite un site et qu'un téléchargement de fichier est lancé sans interaction de l'utilisateur. Cette technique peut être utilisée pour distribuer des logiciels indésirables et des programmes malveillants dans l'espoir que les utilisateurs exécutent accidentellement afin qu'ils soient infectés.

   https://www.bleepingcomputer.com/news/security/web-browsers-still-allow-drive-by-downloads-in-2020/

7. **Hack de Minneapolis Police Department Probablement faux, d'après un chercheur**
   Selon Troy Hunt sur Have I Been Pwned (HIBP), le groupe d'adresses e-mail et de mots de passe prétendument mal acquis circule dans plusieurs forums, la plupart attribuant la fuite d'informations d'identification à Anonymous. Selon plusieurs publications sur les réseaux sociaux, Anonymous aurait commis la brèche en réponse au rôle du MPD dans la mort de Floyd

   https://threatpost.com/anonymous-hack-minneapolis-police-department-fake/156171/

III. 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**.