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 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 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, un contournement de la politique de sécurité et une atteinte à la confidentialité des données. Les versions affectées sont : • Firefox versions antérieures à 78 • Firefox ESR versions antérieures à 68.10	02/07/2020	CVE-2020-12426	78.0.1 Télécharger	Mettre à jour le navigateur	10.0
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 83.0.4103.116	23/06/2020	-	83.0.4103.116 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 problème de sécurité non spécifié par l'éditeur, une exécution de code arbitraire et un déni de service à distance.	29/06/2020	CVE-2020-10757	Contacter SUSE	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20201784-1/	8.4
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance.	01/07/2020	CVE-2020-1457	10	Mettre à jour le système via Windows Update	7.3
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 systèmes affectés sont les suivants : Google Chrome OS versions antérieures à 83.0.4103.119 (platform version: 13020.87.0)	25/06/2020		OS83	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/06/stable-channel-update-for-chrome-os.html	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 et un déni de service. Les systèmes affectés sont les suivants : • Ubuntu 20.04 LTS • Ubuntu 19.10 • Ubuntu 18.04 LTS	26/06/2020	CVE-2020-5973	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4404-2/	-
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 un déni de service, une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes affectés sont les suivants : • MRG Realtime 2 x86_64 • Red Hat Enterprise Linux Server - AUS 6.5 x86_64 • Red Hat Enterprise Linux Server - TUS 7.4 x86_64	01/07/2020	CVE-2018-20169	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:2777	6.8

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 une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une injection de requêtes illégitimes par rebond (CSRF). Les versions affectées sont : • Drupal versions 7.x antérieures à 7.72 • Drupal versions 8.8.x antérieures à 8.8.8 • Drupal versions 8.9.x antérieures à 8.9.1 • Drupal versions 9.x antérieures à 9.0.1	19/06/2020	CVE-2020-13665	9.0.1 Télécharger	Mettre à jour le CMS	-

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 une exécution de code arbitraire et un déni de service. Les versions concernées sont les suivantes : • ESXi 7.x versions antérieures à ESXi_7.0.0-1.20.16321839 • ESXi 6.7.x versions antérieures à ESXi670-202006401-SG • ESXi 6.5.x versions antérieures à ESXi650-202005401-SG • Fusion 11.x versions antérieures à 11.5.5 • Workstation 15.x versions antérieures à 15.5.5 • VMware Cloud Foundation 4.x versions antérieures à 4.0.1 • VMware Cloud Foundation 3.x versions antérieures à 3.10.0.1	24/06/2020	CVE-2020-3971	-	Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2020-0015.html	5.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes infectés sont les suivants : • FortiAnalyzer versions antérieures à 6.0.9 • FortiAnalyzer versions 6.2.x antérieures à 6.2.4 • FortiManager versions antérieures à 6.0.9 • FortiManager versions 6.2.x antérieures à 6.2.4 • FortiAP-S/W2 versions antérieures à 6.2.4 • FortiAP-U versions antérieures à 6.0.2	30/06/2020	CVE-2004-1653	Contacter Fortinet	Veuillez-vous référer au Bulletin de sécurité https://fortiguard.com/psirt/FG-IR-19-292	-
Vulnérabilité dans Wireshark	Une vulnérabilité a été découverte dans Wireshark. Elle permet à un attaquant de provoquer un déni de service à distance Les versions affectées sont les suivantes : Wireshark versions 3.2.x antérieures à 3.2.5	02/07/2020	CVE-2020-15466	3.2.5 Télécharger	Mettre à jour en version 3.2.5 ou ultérieure https://www.wireshark.org/security/wnpa-sec-2020-09.html	-

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 antérieures à 13.1.2, 13.0.8 et 12.10.13	02/07/2020		13.1.2	Veuillez-vous référer au Bulletin de sécurité https://about.gitlab.com/releases/2020/07/01/security-release-13-1-2-release/	-
Vulnérabilité dans McAfee	Une vulnérabilité a été corrigée dans McAfee Advanced Threat Defense (ATD). Un attaquant pourrait exploiter cette vulnérabilité pour visualiser des fichiers sensibles. Les versions affectées sont les suivantes : McAfee Advanced Threat Defense (ATD) version antérieure à 4.10.0	26/06/2020	CVE-2020-7262	Contacter McAfee	Veuillez-vous référer au Bulletin de sécurité https://kc.mcafee.com/corporate/index?page=content&id=SB10319	5.3

II.5 Actualités

1. **Le botnet polyvalent Lucifer enrôle les systèmes Windows**
   Des chercheurs ont découvert un malware, nommé Lucifer, qui attaque des systèmes windows pour les asservir dans un botnet. Ce dernier est polyvalent et pourrait mener à la fois des attaques DDoS ou activer des cryptomineurs.
   https://www.lemondeinformatique.fr/actualites/lire-le-botnet-polyvalent-lucifer-enrole-les-systemes-windows-79577.html

2. **Avec File Recovery, Microsot livre un récupérateur de fichiers pour Windows 10**
   La firme de Redmond a développé l'outil gratuit File Recovery pour Windows 10. Il a pour objectif de récupérer les fichiers supprimés ou perdus.
   https://www.lemondeinformatique.fr/actualites/lire-avec-file-recovery-microsot-livre-un-recuperateur-de-fichiers-pour-windows-10-79580.html

3. **Adobe recommande de désinstaller Flash Player d'ici fin 2020**
   Annoncé il y a près de 3 ans, l'arrêt de la distribution et du support du lecteur Flash d'Adobe est prévu le 31 décembre 2020. Plus aucun contenu en ligne basé sur cette technologie ne pourra être exécuté dans Adobe Flash Player à compter de cette date.
   https://www.lemondeinformatique.fr/actualites/lire-adobe-recommande-de-desinstaller-flash-player-d-ici-fin-2020-79501.html

4. **24 ans de données policières diffusées par des hacktivisites**
   Le groupe de pirates informatiques hacktivistes Distributed Denial of Secrets vient de mettre en ligne 24 ans de documents policiers volés dans 200 services judiciaires de 254 services de police de part le monde.
   https://www.zataz.com/24-ans-de-donnees-policieres-diffusees-par-des-hacktivisites/

5. **CISA : les attaquants des États-nations sont susceptibles d'exploiter le bogue de Palo Alto Networks**
   Une vulnérabilité de contournement de l'authentification permet aux attaquants d'accéder aux actifs du réseau sans informations d'identification lorsque SAML est activé sur certains pare-feu et VPN d'entreprise.
   https://threatpost.com/cisa-nation-state-attackers-palo-alto-networks-bug/157013/

6. **Microsoft Defender ATP peut désormais protéger les appareils Linux et Android**
   Microsoft Defender Advanced Threat Protection (ATP) s'est étendu aux plates-formes non Windows et est désormais généralement disponible pour les entreprises utilisant des appareils Linux et en aperçu public pour ceux qui ont des appareils Android.
   https://www.bleepingcomputer.com/news/security/microsoft-defender-atp-can-now-protect-linux-android-devices/

7. **Les pirates utilisent Google Analytics pour voler des cartes de crédit, contourner le CSP**
   Les pirates utilisent les serveurs de Google et la plate-forme Google Analytics pour voler les informations de carte de crédit soumises par les clients des magasins en ligne.
   https://www.bleepingcomputer.com/news/security/hackers-use-google-analytics-to-steal-credit-cards-bypass-csp/

8. **Les pirates de CryptoCore ont fait plus de 200 millions de dollars violant les échanges de crypto**
   Un groupe de piratage connu sous le nom de CryptoCore a réussi à cambrioler des cambriolages de crypto-monnaie d'une valeur de 70 millions de dollars, mais la recherche indique qu'il pourrait s'agir d'une valeur estimée à plus de 200 millions de dollars depuis 2018.
   https://www.bleepingcomputer.com/news/security/cryptocore-hackers-made-over-200m-breaching-crypto-exchanges/

9. **Près de 300 exécutables Windows 10 vulnérables au piratage de DLL**
   Un simple VBScript peut suffire pour permettre aux utilisateurs d'obtenir des privilèges administratifs et de contourner UAC entièrement sur Windows 10.
   https://www.bleepingcomputer.com/news/security/almost-300-windows-10-executables-vulnerable-to-dll-hijacking/

10. **Les États-Unis désignent Huawei et ZTE en Chine comme menaces à la sécurité nationale**
    La Federal Communications Commission (FCC) des États-Unis a officiellement désigné Huawei Technologies Company (Huawei) et ZTE Corporation (ZTE) comme menaces à la sécurité nationale de l'intégrité des réseaux de communication américains ou de la chaîne d'approvisionnement des communications.

    https://www.bleepingcomputer.com/news/security/us-designates-chinas-huawei-and-zte-as-national-security-threats/

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**.