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'Août 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 Microsoft IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une exécution de code à distance. Les versions affectées sont les suivantes : • Internet Explorer 11 • Internet Explorer 9	12/08/2020	CVE-2020-1570	-	Mettre à jour via Windows Update	-
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 84.0.4147.125	11/08/2020	CVE-2020-6555	84.0.4147.125 Télécharger	Mettre à jour le navigateur	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft EDGE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une élévation de privilèges et une exécution de code à distance. Les versions affectées sont les suivantes : • Microsoft Edge (Chromium-based) • Microsoft Edge (EdgeHTML-based)	12/08/2020	CVE-2020-1569	-	Mettre à jour via Windows Update	6.2

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 un déni de service à distance. Les versions affectées sont les suivantes : Google Android toutes versions sans le correctif de sécurité du 03 août 2020.	04/08/2020	CVE-2020-3647	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/pixel/2020-08-01	-
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 contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS • Ubuntu 14.04 ESM	05/08/2020	CVE-2020-15707	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4432-2	6.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux de Red Hat	Une vulnérabilité a été découverte dans le noyau Linux de Red Hat. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : - MRG Realtime 2 x86_64	04/08/2020	CVE-2019-11487	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:3266	7.8
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer un déni de service, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	11/08/2020	CVE-2020-1587	10	Mettre à jour le système via Windows Update	7.8
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, un déni de service à distance et un contournement de la politique de sécurité	07/08/2020	CVE-2020-15780		Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20202152-1/	6.7

II.3 AUTRES

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 13.2.3, 13.1.6 et 13.0.12	06/08/2020			Veuillez-vous référer au Bulletin de sécurité https://about.gitlab.com/releases/2020/08/05/gitlab-13-2-3-released/	-
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	12/08/2020	CVE-2020-1583	-	Mettre à jour le système via Windows Update	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans McAfee	Plusieurs vulnérabilités ont été corrigées dans McAfee Data Loss Prevention (DLP) ePO extension et McAfee Data Loss Prevention (DLP) pour Mac. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'effectuer des modifications dans la configuration, de réussir une élévation de privilèges ou d'exécuter des commandes à distance.	13/08/2020	CVE-2020-7307	Contacter McAfee	Veuillez-vous référer au Bulletin de sécurité https://kc.mcafee.com/corporate/index?page=content&id=SB10319	5.3
Vulnérabilité dans TeamViewer Desktop	Une vulnérabilité critique a été corrigée dans TeamViewer Desktop pour Windows. La faille « CVE-2020-13699 » pourrait être exploité par un attaquant distant pour déchiffrer le mot de passe des utilisateurs Windows, exécuter du code arbitraire à distance et conduire à une exploitation ultérieure du système affecté. Les systèmes infectés sont les suivants : TeamViewer Desktop pour Windows versions 15.8.x antérieures à 15.8.3,	10/08/2020	CVE-2020-13699	15.8.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://community.teamviewer.com/t5/Announcements/Statement-on-CVE-2020-13699/td-p/98448	8.8

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 un déni de service, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité	12/08/2020	CVE-2020-1591	-	Mettre à jour le système via Windows Update	-
Vulnérabilité dans Microsoft .Net	De multiples vulnérabilités ont été corrigées dans Microsoft .Net. Elles permettent à un attaquant de provoquer un déni de service, une élévation de privilèges et une exécution de code à distance.	12/08/2020	CVE-2020-1597	-	Mettre à jour le système via Windows Update	-
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, un déni de service à distance et une atteinte à la confidentialité des données.	06/08/2020	CVE-2020-3433		Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbss-ipv6-dos-3bLk6vA	7.8

III. ACTUALITÉS

1. **Microsoft Office cible privilégiée pour mener des attaques**
   Les navigateurs devenant des cibles plus difficiles, les cybercriminels s'appuient de plus en plus sur la suite de productivité de Microsoft pour mener leurs attaques. Au cours des deux dernières années, leur nombre a beaucoup augmenté et aujourd'hui la diffusion des logiciels malveillants se fait plus par les fichiers Office que par les PDF.
   https://www.lemondeinformatique.fr/actualites/lire-microsoft-office-cible-privilegiee-pour-mener-des-attaques-79874.html

2. **Protéger son réseau Windows contre les droits d'admin excessifs**
   Chaque développeur ou utilisateur de réseau disposant de privilèges d'administrateur accroît le risque de compromission de compte. D'où l'intérêt de réexaminer les privilèges et de prendre des mesures pour mieux gérer les droits d'accès à son réseau Windows.
   https://www.lemondeinformatique.fr/actualites/lire-proteger-son-reseau-windows-contre-les-droits-d-admin-excessifs-79893.html

3. **Le grand firewall chinois bloque le trafic HTTPS utilisant TLS 1.3**
   Des chercheurs ont découvert que, depuis la fin juillet, la Chine avait commencé à bloquer le trafic HTTPS utilisant le protocole TLS 1.3 et une de ses fonctionnalités, ESNI, l'Encrypted Server Name Indication.
   https://www.lemondeinformatique.fr/actualites/lire-le-grand-firewall-chinois-bloque-le-trafic-https-utilisant-tls-13-79983.html

4. **Interpol analyse l'évolution des cyberattaques liées au Covid-19**
   L'organisation internationale de police criminelle Interpol a rendu un rapport sur les cyberattaques dans le contexte de la pandémie. Sans surprise, le Covid-19 a constitué un effet d'aubaine pour les cybercriminels qui ont multiplié les campagnes de phishing, de ransomwares et d'URL malveillantes.
   https://www.lemondeinformatique.fr/actualites/lire-interpol-analyse-l-evolution-des-cyberattaques-liees-au-covid-19-79925.html

5. **SANS Institute et ISC2, des experts en sécurité victimes de fuites de données**
   Deux sociétés de formation et de certification dans le domaine de la cybersécurité ont été touchées par des fuites de données. SANS Institute l'a été via un phishing et ISC2 à travers un bucket S3 mal configuré.
   https://www.lemondeinformatique.fr/actualites/lire-sans-institute-et-isc2-des-experts-en-securite-victimes-de-fuites-de-donnees-80023.html

6. **La cybersécurité manque de bras faute de formation**
   70% des entreprises manquent de spécialistes en sécurité informatique, indique une enquête mondiale menée par l'ESG, l'ISSA et (ISC)2, précisant qu'il faudrait en former 4 millions pour répondre aux besoins du marché. Les raisons ? Un manque de candidats qualifiés qui freinent les recrutements et des plans de carrière quasi-inexistants après l'intégration dans l'entreprise.
   https://www.lemondeinformatique.fr/actualites/lire-la-cybersecurite-manque-de-bras-faute-de-formation-80016.html

7. **Drovorub : Le MacGyver 2.0 des espions Russes ?**
   Les Services de renseignement Américains et le FBI alertent les entreprises de la découverte d'une arme exploitée par les espions Russes du nom de Drovorub.
   https://www.zataz.com/drovorub-le-macgyver-2-0-des-espions-russes/

8. **Techniques de pirates – Comment les cybercriminels blanchissent l'argent du carding (Cash Out) ?**
   Blanchir l'argent émanant de la cybercriminalité et plus particulièrement du carding est une affaire hautement risquée. Le processus est lourd, long, coûteux et les intermédiaires ne sont pas fiables. Comment procède les pirates aujourd'hui pour réaliser un Cash Out (Ca$h Out) ?
   https://www.undernews.fr/fiches-pirates/techniques-de-pirates-comment-les-cybercriminels-blanchissent-largent-carding-cashout

9. **Le FBI et la NSA exposent un malware Linux utilisé par le renseignement russe**
   Le FBI et la NSA ont publié une alerte de sécurité commune contenant des détails techniques sur un nouveau logiciel malveillant Linux développé par les pirates militaires russes.
   https://www.zdnet.fr/actualites/le-fbi-et-la-nsa-exposent-un-malware-linux-utilise-par-le-renseignement-russe-39908157.htm

10. **Ransomware : voici les indices qui montrent que vous êtes attaqué**
    Les hackers peuvent mettre des mois à préparer des attaques de rançongiciel. Voici ce à quoi il faut faire attention si vous pensez que vous pouvez être une cible.
    https://www.zdnet.fr/pratique/ransomware-voici-les-indices-qui-montrent-que-vous-etes-attaque-39908063.htm

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**.