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 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	Une vulnérabilité a été découverte dans Mozilla Firefox. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont : Firefox pour iOS versions antérieures à 26	02/06/2020	CVE-2020-12404	77.0.1 Télécharger	Mettre à jour le navigateur	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 élévation de privilèges, une exécution de code à distance et une usurpation d'identité. Les versions affectées sont les suivantes : • Microsoft Edge (Chromium) • Microsoft Edge (Chromium) en mode IE Microsoft Edge (EdgeHTML)	10/06/2020	CVE-2020-1242	-	Mettre à jour via Windows Update	9.0

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 atteinte à la confidentialité des données et une exécution de code à distance. Les versions concernées sont les suivantes : • Internet Explorer 11 • Internet Explorer 9	10/06/2020	CVE-2020-1315	-	Mettre à jour le système via Windows Update	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 à distance et un déni de service à distance.	10/06/2020	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 Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer un déni de service, un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, une élévation de privilèges et une exécution de code à distance.	10/06/2020	CVE-2020-1334	10	Mettre à jour le système via Windows Update	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 systèmes affectés sont les suivants : Chrome OS versions antérieures à 83.0.4103.97 (Platform version : 13020.67.0)	04/06/2020		OS83	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/06/stable-channel-update-chrome-os.html	10.0

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 du 4 mai 2020	02/06/2020	CVE-2020-3676	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/pixel/2020-06-01	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 à distance, un contournement de la politique de sécurité 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 • Ubuntu 16.04 LTS • Ubuntu 14.04 ESM • Ubuntu 12.04 ESM	11/06/2020	CVE-2020-12826	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://usn.ubuntu.com/4393-1/	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux de Red Hat	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. 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 une atteinte à la confidentialité des données.	11/06/2020	CVE-2020-10711	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:2522	10.0

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans WordPress	De multiples vulnérabilités ont été découvertes dans WordPress. Certaines d'entre elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur, une atteinte à la confidentialité des données et une élévation de privilèges. Les versions affectées sont : • WordPress versions 5.4.x antérieures à 5.4.2 • WordPress version 5.3 sans le dernier correctif de sécurité	11/06/2020	-	5.4.2 Télécharger	Mettre à jour le CMS	4.5

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Reader et Acrobat	Une vulnérabilité a été découverte dans Adobe Flash Player. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance Les versions affectées sont les suivantes : • Adobe Flash Player Desktop Runtime versions antérieures à 32.0.0.387 sur Windows et macOS • Adobe Flash Player pour Google Chrome versions antérieures à 32.0.0.387 sur Windows, macOS, Linux et Chrome OS • Adobe Flash Player pour Microsoft Edge et Internet Explorer 11 versions antérieures à 32.0.0.387 sur Windows 10 et 8.1 • Adobe Flash Player Desktop Runtime versions antérieures à 32.0.0.387 sur Linux	10/06/2020	CVE-2020-9633	Télécharger Adobe	Veuillez-vous référer au guide de sécurité pour obtenir les correctifs https://helpx.adobe.com/security/products/flash-player/apsb20-30.html	8.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits VMware	Une vulnérabilité a été découverte dans les produits VMware. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions concernées sont les suivantes : • ESXi versions 6.7.x antérieures à ESXi670-202006401-SG • ESXi versions 6.5.x antérieures à ESXi650-202005401-SG • Workstation versions antérieures à 15.5.5 • Fusion versions antérieures à 11.5.5	12/06/2020	CVE-2020-3960		Veuillez-vous référer au Bulletin de sécurité https://www.vmware.com/security/advisories/VMSA-2020-0012.html	10.0
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 13.0.6, 12.10.11 et 12.9.10	11/06/2020			Veuillez-vous référer au Bulletin de sécurité https://about.gitlab.com/releases/2020/06/10/critical-security-release-13-0-6-released/	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et une usurpation d'identité.	10/06/2020	CVE-2020-1323	2019	Mettre à jour le système via Windows Update	7.7
Vulnérabilité dans Bitdefender	Une vulnérabilité de mauvaise gestion des liens symboliques a été corrigée dans la version gratuite de l'antivirus Bitdefender. L'exploitation de cette faille peut permettre à un attaquant de manipuler (remplacer, restaurer) des fichiers mis en quarantaine.	11/06/2020	CVE-2020-8103	Contacter Bitdefender	Veuillez-vous référer au Bulletin de sécurité https://www.bitdefender.com/support/security-advisories	7.2

II.5 Actualités

1. **Thanos : Le premier rançongiciel avec technique d'évasion RIPlace anti-ransomware**
   Le ransomware Thanos découvert en janvier 2020 est le premier à utiliser une technique d'évasion anti-ransomware baptisée RIPlace comme l'a révélé les chercheurs en sécurité de Inskit Group qui ont publiés une analyse du malware mettant en avant de nombreuses autres fonctionnalités avancées qui en font une menace sérieuse à surveiller. Il est capable de détecter et de désactiver de nombreux logiciel de sécurité comme les anti-ransomwares, les antivirus ou encore les pare-feu
   https://www.undernews.fr/malwares-virus-antivirus/thanos-le-premier-rancongiciel-avec-technique-devasion-riplace-anti-ransomware.html

2. **Fraude sur YouTube : Ils se font passer pour Elon Musk de SpaceX et volent 150 000$ en BTC**
   Voilà le parfait scénario d'arnaque via des vidéos YouTube. Les pirates ont réussi à rafler une belle mise en Bitcoin en un temps record. Les escrocs ont réussi à inciter les internautes à envoyer une petite quantité de Bitcoin et à en obtenir le double en retour en se faisant passer pour Elon Musk et son projet SpaceX.
   https://www.undernews.fr/hacking-hacktivisme/fraude-sur-youtube-ils-se-font-passer-pour-elon-musk-de-spacex-et-volent-150-000-en-btc.html

3. **Patch Tuesday : 128 vulnérabilités dont 11 critiques corrigés en juin**
   Le mois de juin aura connu son GROS lot de corrections de vulnérabilité pour les produits Microsoft et Adobe. 128 vulnérabilités dont 11 critiques notamment pour SharePoint et les postes de travail dans la ligne de mire.
   https://www.zataz.com/patch-tuesday-128-vulnerabilites-dont-11-critiques-corriges-en-juin/

4. **Un partenaire de la NASA piraté, des données divulguées**
   La société américaine Digital Management, partenaire technologique de la NASA piratée. Les malveillants diffusent plusieurs milliers de fichiers confidentiels.
   https://www.zataz.com/un-partenaire-de-la-nasa-pirate-des-donnees-divulguees/

5. **Les pirates de Bolloré diffusent des données**
   Le 24 mai 2020 je vous expliquais l'implication des pirates informatiques cachés derrière le ransomware NetWalker dans le piratage et la mise en place d'un chantage numérique à l'encontre de la société Bolloré. Les malveillants avaient infiltré une filiale du groupe français : Transport et Logistics en République Démocratique du Congo (RDC). Ce groupe a automatisé l'ensemble de son processus malfaisant. Il infiltre, dérobe un maximum de documents, lance le chiffrement des machines. Finalité, réclamer une rançon.
   https://www.zataz.com/les-pirates-de-bollore-diffusent-des-donnees/

6. **Lamphone: espionner à partir d'une lampe**
   Des chercheurs en sécurité de l'Université Ben-Gourion et du Weizmann Institute of Science ont dévoilé un vecteur de cyberattaque aussi innovant qu'inattendu dont le procédé passe par la lumière d'une ampoule.
   https://www.lemondeinformatique.fr/actualites/lire-lamphone-espionner-a-partir-d-une-lampe-79428.html

7. **Alerte WFH : bogue critique détecté dans les anciens modèles de routeurs D-Link**
   Les chercheurs découvrent six bogues dans le routeur cloud double bande sans fil AC 1750 DIR-865L D-Link.
   https://threatpost.com/work-from-home-alert-critical-d-link-bug/156573/

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**.