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 Juillet 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. 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 contournement de la politique de sécurité. Les versions affectées sont : • Firefox versions antérieures à 79 • Firefox ESR versions antérieures à 68.11 • Firefox ESR versions antérieures à 78.1 • Firefox iOS versions antérieures à 28	29/07/2020	CVE-2020-15662	79 Télécharger	Mettre à jour le navigateur	-

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 84.0.4147.105	28/07/2020	CVE-2020-6541	84.0.4147.105 Télécharger	Mettre à jour le navigateur	-
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	20/07/2020	CVE-2020-1341	-	Mettre à jour via Windows Update	-

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. 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 : • SUSE Linux Enterprise Server 15 • SUSE Linux Enterprise Server 12 • SUSE Linux Enterprise Server 11	30/07/2020	CVE-2020-15706		Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/kb/doc/?id=000019673	6.4
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	30/07/2020	CVE-2020-15707	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4432-1	6.4

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 une exécution de code arbitraire, un déni de service à distance et un contournement de la politique de sécurité.	30/07/2020	CVE-2020-15780	8.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:3228	6.7
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 84.0.4147.110 (Platform version : 13099.85.0)	30/07/2020		OS84	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/07/stable-channel-update-chrome-os_29.html	-

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla	De multiples vulnérabilités ont été découvertes dans Joomla. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à l'intégrité des données, une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Les versions affectées sont : • Joomla versions antérieures à 3.9.20	17/07/2020	CVE-2020-15699	3.9.20 Télécharger	Mettre à jour le CMS	5.3
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 déni de service à distance et une élévation de privilèges. Les versions affectées sont : • Moodle versions 3.9.x antérieures à 3.9.1 • Moodle versions 3.8.x antérieures à 3.8.4 • Moodle versions 3.7.x antérieures à 3.7.7 • Moodle versions antérieures à 3.5.13	17/07/2020	CVE-2020-14322	3.9.1 Télécharger	Mettre à jour le CMS	6.7

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Thunderbird	De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Certaines d'entre 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. Les versions concernées sont les suivantes : • Thunderbird versions antérieures à 68.11	31/07/2020	CVE-2020-15659	78.1.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.mozilla.org/en-US/security/advisories/mfsa2020-35/	9.0
Vulnérabilité dans Foxit Reader et PhantomPDF	De multiples vulnérabilités ont été découvertes dans Foxit Reader et PhantomPDF. 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 infectés sont les suivants : • Foxit Reader versions antérieures à 10.0.0.35798 • Foxit PhantomPDF versions antérieures à 10.0.0.35798	31/07/2020	CVE-2020-12248	10.0.0.35798 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.foxitsoftware.com/support/security-bulletins.html	4.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Zimbra	De multiples vulnérabilités ont été découvertes dans Zimbra. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Zimbra versions 9.0.0.x antérieures à 9.0.0 Patch 5 • Zimbra versions 8.8.15.x antérieures à 8.8.15 Patch 12	28/07/2020	CVE-2019-1010091	9.0.0 P5 Télécharger	Mettre à jour en version 3.2.5 ou ultérieure https://blog.zimbra.com/2020/07/new-zimbra-patches-9-0-0-patch-5-and-8-8-15-patch-12/	6.1
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 contournement de la politique de sécurité et une atteinte à l'intégrité des données.	31/07/2020	CVE-2020-3386		Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-devmgr-cmd-inj-Umc8RHNh	8.8
Vulnérabilité dans les produits Kaspersky	De multiples vulnérabilités ont été découvertes dans les produits Kaspersky. Elles permettent à un attaquant de provoquer un déni de service à distance et une élévation de privilèges.	29/07/2020			Veuillez-vous référer au Bulletin de sécurité https://support.kaspersky.com/general/vulnerability.aspx?el=12430#290720	7.1

III. ACTUALITÉS

1. **Top mondial des Etats les plus touchés par des cyberattaques**
   Au cours des 14 dernières années, les trois Etats les plus touchés par des cyberattaques significatives au niveau mondial ont été les Etats-Unis, le Royaume-Uni et l'Inde d'après une enquête menée par Specops ayant analysé les données issues du CSIS. La France pointe à la 14e place ex-aequo avec Israël.
   https://www.lemondeinformatique.fr/actualites/lire-top-mondial-des-etats-les-plus-touches-par-des-cyberattaques-79788.html

2. **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…
   https://www.lemondeinformatique.fr/actualites/lire-microsoft-office-cible-privilegiee-pour-mener-des-attaques-79874.html

3. **Trump confirme une cyber attaque à l'encontre d'une entreprise Russe**
   Le Président Américain, Donald Trump, a confirmé une cyber attaque à l'encontre d'une entreprise Russe accusée d'être à l'origine de centaines de fake news.
   https://www.zataz.com/trump-confirme-une-cyber-attaque-a-lencontre-dune-entreprise-russe/

4. **La nouvelle loi française sur le porno est une menace pour la cybersécurité**
   Avec l'adoption de la nouvelle loi sur la violence domestique, le gouvernement français a commencé à accorder une attention beaucoup plus grande aux sites web pour adultes. Emmanuel Macron considère que la politique actuelle en matière de contenu pour adultes est inacceptable, c'est pourquoi les sites pornographiques attendent une succession de changements. Selon le président, les propriétaires de services au contenu destiné aux plus de 18 ans ne prennent pas suffisamment de mesures pour protéger les enfants.
   https://www.undernews.fr/anonymat-cryptographie/la-nouvelle-loi-francaise-sur-le-porno-est-une-menace-pour-la-cybersecurite.html

5. **Facebook crée un Facebook alternatif où des bots essayent d'arnaquer d'autres bots**
   Facebook crée un Facebook alternatif où des bots
   https://cyberguerre.numerama.com/6563-facebook-cree-un-facebook-alternatif-ou-des-bots-essayent-darnaquer-dautres-bots.html

6. **HaveIBeenPwned dépasse les 10 milliards d'identifiants volés : testez les vôtres !**
   HaveIBeenPwned dépasse les 10 milliards.
   https://cyberguerre.numerama.com/6361-haveibeenpwned-depasse-les-10-milliards-didentifiants-voles-testez-les-votres.html

7. **Open Source Security Foundation : regrouper pour mieux sécuriser**
   Open Source : Une nouvelle fondation vient rassembler les différents efforts de la communauté visant à mieux sécuriser les programmes Open Source.
   https://www.zdnet.fr/actualites/open-source-security-foundation-regrouper-pour-mieux-securiser-39907689.htm

8. **Google : Onze failles 0day exploitées par des cybercriminels au 1er semestre 2020**
   Un rapport du Projet Zero de Google examine les statistiques de 2019 et 2020 sur les failles 0day et en tire des conclusions intéressantes.
   https://www.zdnet.fr/actualites/google-onze-failles-0day-exploitees-par-des-cybercriminels-au-1er-semestre-2020-39907625.htm

9. **Piratage de Twitter : retour sur la chasse à l'homme lancée par le FBI**
   Après plusieurs jours d'une chasse à l'homme mouvementée, les autorités américaines ont finalement réussi à mettre la main sur les auteurs présumés du piratage de Twitter. Retour sur une traque hors du commun.
   https://www.zdnet.fr/actualites/piratage-de-twitter-retour-sur-la-chasse-a-l-homme-lancee-par-le-fbi-39907605.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**.