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 d'Octobre 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 et une exécution de code arbitraire à distance. Les versions affectées sont : Google Chrome versions antérieures à 86.0.4240.75	21/10/2020	CVE-2020-16003	86.0.4240.75 Télécharger	Mettre à jour le navigateur	8.8
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Foundation 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 et un déni de service. Les versions affectées sont les suivantes : • Firefox versions antérieures à 82 • Firefox ESR versions antérieures à 78.4	21/10/2020	CVE-2020-15684	82 Télécharger	Mettre à jour le navigateur	9.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Edge	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur et une exécution de code arbitraire à distance. La version affectée est la suivante : Edge versions antérieures à 86.0.622.51	27/10/2020	-	86.0.622.51	Mettre à jour le système via Windows Update	-

II.2 Systèmes d'exploitation

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	Des chercheurs en cybersécurité ont révélé l'existence d'une vulnérabilité Zero-day dans le système d'exploitation Windows. Cette faille touche "Windows Kernel Cryptography Driver" (cng.sys). Elle peut être exploitée par un attaquant local pour réussir une élévation de privilèges. Toutes les versions de Windows sont affectées.	02/11/2020	CVE-2020-17087	10	Le zero-day devrait être corrigé le 10 novembre 2020, date du prochain correctif de Microsoft. Mettre à jour le système via Windows Update	-
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 physiquement proche de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données. Les systèmes infectés sont les suivants : • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS	20/10/2020	CVE-2020-24490	20.04.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4591-1	-

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, une exécution de code arbitraire à distance et un déni de service à distance.	04/11/2020	CVE-2020-24490	8.3.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:4686	-
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 et un déni de service. Les versions infectées sont les suivantes : Google Android toutes versions maintenues sans le correctif à venir le 05 novembre 2020	03/11/2020	CVE-2020-0454	11	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2020-11-01	5.5
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 à distance et une atteinte à la confidentialité des données. L'exploitation de certaines de ces vulnérabilités nécessite une proximité physique avec le système vulnérable.	21/10/2020	CVE-2020-12352	15	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20202972-1/	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Debian LTS	De multiples vulnérabilités ont été découvertes dans Debian LTS. 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. Les systèmes infectés sont les suivants : • Debian 9 Stretch versions antérieures à 4.9.240-1	30/10/2020	CVE-2020-26088	10.6.0	Veuillez-vous référer au Bulletin de sécurité https://www.debian.org/lts/security/2020/dla-2420	5.5
Vulnérabilité dans Google Chrome OS	De multiples vulnérabilités ont été découvertes dans 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 86.0.4240.112 (Platform version: 13421.73.0)	23/10/2020	-	OS86	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-chrome-os_22.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GoogleChromeReleases+%28Google+Chrome+Releases%29	-

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Pulse Secure	De multiples vulnérabilités ont été découvertes dans les produits Pulse Secure. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données.	27/10/2020	CVE-2020-13162	-	Veuillez-vous référer au Bulletin de sécurité https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601/?kA23Z000000boS0	7.0
Vulnérabilités dans les produits IBM	De multiples vulnérabilités ont été découvertes dans les produits IBM. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les versions affectées sont les suivantes : Websphere Application Server versions 7.0, 8.0, 8.5, et 9.0	23/10/2020	CVE-2020-4578	-	Veuillez-vous référer au Bulletin de sécurité https://www.ibm.com/support/pages/node/6351443	5.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Cisco	De multiples vulnérabilités ont été découvertes dans les produits Cisco. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.	22/10/2020	CVE-2020-3572	-	Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-tcp-dos-N3DMnU4T	8.6
Vulnérabilité dans Mozilla Thunderbird	De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance.	21/10/2020	CVE-2020-15969	78.4	Veuillez-vous référer au Bulletin de sécurité https://www.mozilla.org/en-US/security/advisories/mfsa2020-47/	8.8

III. ACTUALITÉS

1. **Windows, plus grande cyber-menace pour les élections américaines de 2020 ?**
   La date du 3 novembre, jour de l'élection présidentielle américaine, approche à grands pas, et l'imminence d'attaques basées sur Windows semble évidente. D'ailleurs, il n'est pas impossible que leur préparation ait probablement commencé. Alors, les graines du chaos ont-elles déjà été semées ?
   https://www.lemondeinformatique.fr/actualites/lire-windows-plus-grande-cyber-menace-pour-les-elections-americaines-de-2020-80757.html

2. **Top25 NSA des failles les plus exploitées par les pirates chinois**
   Pour aider les agences gouvernementales et de la défense américaines à lutter contre les cyberattaquants, la NSA a publié la liste des 25 vulnérabilités les plus exploitées par des pirates chinois.
   https://www.lemondeinformatique.fr/actualites/lire-top25-nsa-des-failles-les-plus-exploitees-par-les-pirates-chinois-80784.html

3. **50% des failles encore ouvertes 6 mois après l'identification**
   Le dernier rapport SOSS de Veracode sur la sécurité des logiciels met en évidence les faiblesses de la chaîne de correction des failles logicielles. Son analyse porte sur 130 000 applications.
   https://www.lemondeinformatique.fr/actualites/lire-50-des-failles-encore-ouvertes-6-mois-apres-l-identification-80853.html

4. **Phishing : des campagnes à grande échelle automatisée par l'intelligence artificielle**
   Si l'utilisation de l'intelligence artificielle à des fins de cyberdéfense est au centre des attentions, il ne faut pas oublier que cette technologie peut aussi être exploitée par les cybercriminels. L'un des domaines ayant récemment connu des avancées surprenantes est celui de la génération de langage naturel. Le centre de recherches privé OpenAI a notamment.
   https://www.silicon.fr/avis-expert/phishing-des-campagnes-a-grande-echelle-automatisee-par-lintelligence-artificielle

5. **Le péché très peu mignon des apps**
   Je me suis essayé au reverse engineering d'une application du top 100 de l'App Store, le résultat n'est pas décevant. Ou plutôt, il est navrant. Chronique de sécurité, le péché très peu mignon des applications mobiles.

   https://www.silicon.fr/avis-expert/securite-le-peche-tres-peu-mignon-des-apps

6. **Islam radical : vague de cyberattaques sur de nombreux sites web français**
   Des hackers ont défiguré des dizaines de petits sites web, en remplaçant leurs homepages par des messages anti-français. Certains détournements sont toujours actifs.
   https://www.01net.com/actualites/islam-radical-vague-de-cyberattaques-sur-de-nombreux-sites-web-francais-1996805.html

7. **Ransomware chez Sopra Steria : Ryuk dénoncé, et maintenant ?**
   Sopra Steria ouvre – un peu – la communication sur la cyberattaque dont il s'est déclaré victime. Une « version inconnue » du ransomware Ryuk est impliquée.
   https://www.silicon.fr/ransomware-sopra-steria-ryuk-349969.html

8. **Les backdoors de la NSA restent un secret bien gardé**
   Un sénateur américain voulait en savoir plus sur la manière dont l'agence américaine implémentait désormais ses portes dérobées dans les technologies américaines. Sans surprise, il n'a pas eu de réponse.
   https://www.01net.com/actualites/les-backdoors-de-la-nsa-restent-un-secret-bien-garde-1998209.html

9. **De nouveau, une série d'applis malveillantes découverte sur Google Play Store**
   Une vingtaine de jeux vidéo installaient en réalité un malware qui bombardait sans relâche les utilisateurs de publicités frauduleuses.
   https://www.01net.com/actualites/de-nouveau-une-serie-d-applis-malveillantes-decouverte-sur-google-play-1997221.html

10. **Le site de campagne de Donald Trump victime d'un défacement**
    Des hackers ont incité les internautes à envoyer des moneros en échange d'une révélation soi-disant sensationnelle sur le coronavirus.
    https://www.01net.com/actualites/le-site-de-campagne-de-donald-trump-victime-d-un-defacement-1997553.html

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**.