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'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. Les versions affectées sont : Google Chrome versions antérieures à 86.0.4240.75	10/10/2020	CVE-2020-15992	86.0.4240.75 Télécharger	Mettre à jour le navigateur	-

II.2 SYSTÈMES D'EXPLOITATION

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, un déni de service, un contournement de la politique de sécurité 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 • Ubuntu 14.04 ESM • Ubuntu 12.04 ESM	14/10/2020	CVE-2020-26088	20.04.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4580-1	5.5
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 une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes affectés sont les suivants : • Red Hat Enterprise Linux Server TUS 7.7 x86_6	13/10/2020	CVE-2019-19527	8.3.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:4236	6.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service, une usurpation d'identité, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	14/10/2020	CVE-2020-16980	10	Mettre à jour le système via Windows Update	7.8
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.	14/10/2020	-	OS85	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-chrome-os.html	-
Vulnérabilité dans Linux Kernel	Une vulnérabilité a été corrigée dans Linux Kernel version antérieure à 5.9-rc4. L'exploitation de cette faille permet à un attaquant de réussir une élévation de privilèges « root » à partir de processus s'exécutant avec des privilèges utilisateur et de porter atteinte à la confidentialité et l'intégrité des données. Les versions infectées sont les suivantes : Linux kernel version antérieure à 5.9-rc4	12/10/2020	CVE-2020-14386	5.9-rc4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=acf69c946233259ab4d64f8869d4037a198c7f06	7.8

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 un déni de service, un contournement de la politique de sécurité et une atteinte à l'intégrité des données.	14/10/2020	CVE-2020-26088	15.2	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20202908-1/	5.5

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Flash Player	De multiples vulnérabilités ont été découvertes dans Adobe Flash Player. Elles permettent à un attaquant de provoquer une exécution de code arbitraire. Les versions affectées sont les suivantes : • Adobe Flash Player Desktop Runtime sur Windows, macOS et Linux versions antérieures à 32.0.0.445 • Adobe Flash Player pour Google Chrome sur Windows, macOS, Linux et Chrome OS versions antérieures à 32.0.0.445 • Adobe Flash Player pour Microsoft Edge et Internet Explorer 11 sur Windows 10 et 8.1 versions antérieures à 32.0.0.445	14/10/2020	CVE-2020-9746	32.0.0.445 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://helpx.adobe.com/security/products/flash-player/apsb20-58.html	7.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	Une vulnérabilité a été corrigée dans Microsoft .Net. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données.	14/10/2020	CVE-2020-19937		Mettre à jour le système via Windows Update	-
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service, une usurpation d'identité, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	14/10/2020	CVE-2020-16957	2019	Mettre à jour le système via Windows Update	7.8
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été corrigées dans les produits Microsoft. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données, un déni de service, une usurpation d'identité, un contournement de la fonctionnalité de sécurité et une exécution de code à distance.	14/10/2020	CVE-2020-17003	-	Mettre à jour le système via Windows Update	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans phpMyAdmin	De multiples vulnérabilités ont été découvertes dans phpMyAdmin. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS) et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • phpMyAdmin versions 4.9.x versions antérieures à 4.9.6 • phpMyAdmin versions 5.0.x versions antérieures à 5.0.3	10/10/2020	CVE-2020-26935	5.0.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.phpmyadmin.net/security/PMASA-2020-6/	-
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 une exécution de code arbitraire, un déni de service et un contournement de la politique de sécurité.	08/10/2020	CVE-2020-3544	-	Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-teams-dll-drsnH5AN	8.8

III. ACTUALITÉS

1. **VMware renforce la sécurité de ses produits réseau SASE et SD-WAN**
   Grâce à des partenariats stratégiques et des rachats pertinents, VMware complète ses offres SASE et SD-WAN et renforce les capacités de sécurité de son SDN NSX.
   https://www.lemondeinformatique.fr/actualites/lire-vmware-renforce-la-securite-de-ses-produits-reseau-sase-et-sd-wan-80554.html

2. **GitHub scanne le code à la recherche de failles**
   Les utilisateurs de GitHub peuvent s'appuyer sur des requêtes prêtes à l'emploi et personnalisées pour trouver les vulnérabilités de sécurité dans leurs bases de code.
   https://www.lemondeinformatique.fr/actualites/lire-github-scanne-le-code-a-la-recherche-de-failles-80579.html

3. **Microsoft corrige 87 failles en octobre dont 11 critiques**
   La mise à jour de sécurité de Microsoft vient d'arriver pour octobre, moins fournie que les autres mois mais avec, comme toujours, des correctifs à installer en priorité. Parmi les 11 failles critiques, celle de la pile TCP/IP est à considérer en premier en raison du risque de propagation d'attaque qu'elle présente.
   https://www.lemondeinformatique.fr/actualites/lire-microsoft-corrige-87-failles-en-octobre-dont-11-critiques-80717.html

4. **L'outil dédié aux examens ProctorU piraté**
   Le site dédié aux passages d'examens en ligne ProctorU infiltré. Le pirate a extrait la base de données. Plus de 400 000 internautes impactés par cette fuite malveillante.
   https://www.zataz.com/loutil-dedie-aux-examens-proctoru-pirate/

5. **Sécuriser le travail à distance : les entreprises cherchent l'équilibre**
   La surface d'attaque s'étend avec la massification du travail à distance et la dispersion des effectifs. Un défi de plus à relever pour les entreprises.

   https://www.silicon.fr/securiser-le-travail-a-distance-les-entreprises-cherchent-lequilibre-349056.html

6. **On pouvait faire planter un PC Windows 10 avec un simple paquet IP**
   Une faille critique a été découverte dans l'implémentation du protocole ICMP. Elle peut facilement provoquer un « écran bleu de la mort ». Mais l'exécution de code arbitraire serait également possible. La vulnérabilité a heureusement été patchée par Microsoft.
   https://www.01net.com/actualites/on-pouvait-faire-planter-un-pc-windows10-avec-un-simple-paquet-ip-1990808.html

7. **Zoom propose enfin le chiffrement de bout en bout**
   Cette nouvelle option de sécurité est disponible dans les prochains jours pour tous les utilisateurs de ce service de visioconférence. Mais elle limite les réunions à 200 participants
   https://www.01net.com/actualites/zoom-propose-enfin-le-chiffrement-de-bout-en-bout-1991386.html

8. **Qakbot : quand les malwares usurpent Windows Defender**
   Le trojan Qakbot a depuis peu un nouveau vecteur de diffusion : un fichier Excel qui contient une alerte semblant émaner de Windows Defender.
   https://www.silicon.fr/qakbot-malwares-windows-defender-349041.html

9. **Android Ransomware a ramassé de nouvelles astuces inquiétantes**
   Bien qu'il soit encore beaucoup plus courant sur les PC, les ransomwares mobiles ont subi une évolution inquiétante, selon de nouvelles recherches.
   https://www.wired.com/story/android-ransomware-worrying-evolution/

10. **Sept grandes démocraties réclament des backdoors pour espionner les messageries chiffrées**
    Le chiffrement de bout en bout reste un gros caillou dans la chaussure des forces de l'ordre qui veulent contraindre les éditeurs à développer des moyens de contournement.
    https://www.01net.com/actualites/sept-grandes-democraties-reclament-des-backdoors-pour-espionner-les-messageries-chiffrees-1989890.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**.