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 Septembre 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 pour Windows, Mac et Linux versions antérieures à 85.0.4183.121	23/09/2020	-	85.0.4183.121 Télécharger	Mettre à jour le navigateur	-
Vulnérabilité dans Apple Safari	De multiples vulnérabilités ont été découvertes dans Apple Safari. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Safari versions antérieures à 14.0	24/09/2020	CVE-2020-9983	14.0	Mettre à jour le navigateur	-

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. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à l'intégrité des données et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Firefox versions antérieures à 81 • Firefox ESR versions antérieures à 78.3 • Thunderbird de version antérieure à 78.3	23/09/2020	CVE-2020-15678	81 Télécharger	Mettre à jour le navigateur	8.8

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. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service et une atteinte à la confidentialité des données.	22/09/2020	CVE-2020-25212	20.04.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4527-1	7.0
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 un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Red Hat Enterprise Linux Workstation 7 x86_64 • Red Hat Enterprise Linux for Real Time 7 x86_64 • Red Hat Enterprise Linux for Real Time for NFV 7 x86_64	30/09/2020		8.3.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://access.redhat.com/errata/RHSA-2020:4060	7.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Apple MacOs	De multiples vulnérabilités ont été découvertes dans Apple MacOS. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à l'intégrité des données et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • macOS High Sierra versions antérieures à 10.13.6 • macOS Mojave versions antérieures à 10.14.6 Update 2020-005 • macOS Catalina versions antérieures à 10.15.7 Update 2020-005	25/09/2020		Contacter Apple	Veuillez-vous référer au Bulletin de sécurité https://support.apple.com/fr-fr/HT211849	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 : Google Chrome OS versions antérieures à 85.0.4183.133 (Platform version : 13310.93.0)	29/09/2020	-	OS85	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/09/stable-channel-update-for-chrome-os_28.html	6.2

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 déni de service, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.	16/09/2020	CVE-2020-24394	15.2	Veuillez-vous référer au Bulletin de sécurité https://www.suse.com/support/update/announcement/2020/suse-su-20202631-1/	7.1

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Elles permettent à un attaquant de provoquer un déni de service, un contournement de la politique de sécurité et une injection de code indirecte à distance (XSS). Les versions affectées sont : • Moodle 3.9 versions antérieures à 3.9.2 • Moodle 3.8 versions antérieures à 3.8.5 • Moodle 3.7 versions antérieures à 3.7.8	21/09/2020	CVE-2020-25631	3.9.2 Télécharger	Mettre à jour le CMS	4.1
Vulnérabilité dans Drupal core	De multiples vulnérabilités ont été découvertes dans Drupal core. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). L'éditeur ne maintient plus les versions 8.x antérieures à 8.8. Les utilisateurs d'une version obsolète doivent préalablement mettre à jour Drupal pour bénéficier des correctifs de sécurité. Les versions affectées sont les suivantes : • Drupal 7.x versions antérieures à	16/09/2020	CVE-2020-13670	9.0.6 Contacter Drupal	Mettre à jour le CMS	8.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	7.73 • Drupal 8.8.x versions antérieures à 8.8.10 • Drupal 8.9.x versions antérieures à 8.9.6 • Drupal 9.0.x versions antérieures à 9.0.6					

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 élévation de privilèges. Les versions infectées sont les suivants : • Foxit Reader versions antérieures à 10.1 • Foxit PhantomPDF versions antérieures à 10.1	28/09/2020	CVE-2020-8758	10.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.foxitsoftware.com/support/security-bulletins.html	4.8
Vulnérabilité dans OpenSSH	De multiples vulnérabilités ont été découvertes dans OpenSSH. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité. Les versions infectées sont les suivantes : • OpenSSH versions antérieures à 8.4	28/09/2020		8.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.openssh.com/txt/release-8.4	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • Wireshark 3.2.x versions antérieures à 3.2.7 • Wireshark 3.0.x versions antérieures à 3.0.14 • Wireshark 2.6.x versions antérieures à 2.6.20	24/09/2020	CVE-2020-25866	3.2.7 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.wireshark.org/security/wnpa-sec-2020-11.html	5.5
Vulnérabilité dans le serveur Samba	L'éditeur du logiciel Samba indique que le serveur Samba est vulnérable à l'attaque ZeroLogon qui touche le protocole Netlogon de Microsoft s'il est configuré en tant que contrôleur de domaine. La vulnérabilité affecte toutes les versions antérieures à v4.8 de Samba configurées en tant que contrôle de domaine (mode 'NT4' ou Active Directory). L'exploitation de cette vulnérabilité permet à un attaquant de réussir une élévation de privilège sur le serveur Samba.	21/09/2020	CVE-2020-1472	4.13.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://www.samba.org/samba/history/samba-4.12.7.html	10.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Cisco	De multiples vulnérabilités ont été découvertes dans certains produits Cisco. Elles permettent à un attaquant de provoquer une élévation de privilèges. Se référer aux informations fournies par le logiciel Cisco Software Checker pour confirmer si les versions logicielles en usage dans le système d'information sont affectées ou non. Les systèmes affectés sont les suivants : • Cisco IOS XE avec le serveur HTTP activé • Logiciel ROMMON	24/09/2020	CVE-2020-3524	-	Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-webui-priv-esc-K8zvEWM	6.4

III. ACTUALITÉS

1. **179 criminels arrêtés sur le dark web**
   Dans une opération d'envergure menée par la police allemande en lien avec Europol et Eurojust avec le soutien des forces de police néerlandaise et agences gouvernementales américaines, 179 escrocs ont été épinglés sur le dark web. Plus de 6 millions d'euros de marchandises ont été saisies.
   https://www.lemondeinformatique.fr/actualites/lire-179-criminels-arretes-sur-le-dark-web-80499.html

2. **Les codes sources de plusieurs Windows, dont XP, divulgués**
   Un leaker aurait mis en ligne sur un forum 4Chan les codes source de très nombreux anciens systèmes d'exploitation Windows, incluant XP, Server 2003 et MS DOS 6.0. Une mise à disposition qui pourrait engendrer des exploits en chaîne.
   https://www.lemondeinformatique.fr/actualites/lire-les-codes-sources-de-plusieurs-windows-dont-xp-divulgues-80495.html

3. **Télétravail : L'usage des équipements personnels augmentent les risques de sécurité**
   Une étude réalisée par Trend Micro durant la crise sanitaire confirme que le télétravail accroît les risques en matière de cybersécurité, en pointant plusieurs pratiques problématiques. Les RSSI ont donc quelques bonnes raisons de se méfier.
   https://www.lemondeinformatique.fr/actualites/lire-teletravail-l-usage-des-equipements-personnels-augmentent-les-risques-de-securite-80491.html

4. **La faille Zerologon fait trembler le département de la sécurité intérieure US**
   La vulnérabilité CVE-2020-1472 surnommée Zerologon permettant à un pirate de prendre le contrôle d'un domaine Windows via le protocole Netlogon a fait sortir de ses gonds le département de la sécurité intérieure aux Etats-Unis. Les DSI des agences gouvernementales n'ayant pas appliqué le correctif de Mcrosoft au plus tard le 1er octobre 2020 seront sanctionnés.
   https://www.lemondeinformatique.fr/actualites/lire-la-faille-zerologon-fait-trembler-le-departement-de-la-securite-interieure-us-80461.html

5. **Le détournement de salaires attire aussi les pirates**
   Le détournement de salaires, une cyber menace en plein essor. 35 000 tentatives de détournement de salaire par courriels piégés bloqués au 1er semestre 2020. Le FBI notait, en 2019, une augmentation de 815 % de la pratique !

   https://www.zataz.com/le-detournement-de-salaires-attire-aussi-les-pirates/

6. **Mise en vente de plus de 10 000 sites web piratés**
   Des pirates informatiques mettent en vente les contenus volés à plus de 10 000 sites web. Les bases de données et les internautes vendus entre 10 et 1 000 $.
   https://www.zataz.com/mise-en-vente-de-plus-de-10-000-sites-web-pirates/

7. **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/

8. **Une cyberattaque paralyse à elle seule le fonctionnement de plusieurs centaines d'hôpitaux américains**
   La chaîne d'hôpitaux américaine Universal Health Services doit faire face à une cyberattaque d'ampleur, qui paralyse le fonctionnement de tout le matériel informatique d'une majorité de ses 400 hôpitaux.
   https://cyberguerre.numerama.com/7985-une-cyberattaque-paralyse-a-elle-seule-le-fonctionnement-de-plusieurs-centaines-dhopitaux-americains.html

9. **5 outils pour prendre le pouls des menaces**
   Chaque entreprise adopte des solutions différentes pour gérer les vulnérabilités. Cela va de la formation des personnels et de la mise en oeuvre des meilleures pratiques jusqu'au aux outils de gestion spécifiques. Retour sur 5 solutions capables de hiérarchiser les risques.
   https://www.lemondeinformatique.fr/actualites/lire-cybersecurite-5-outils-pour-prendre-le-pouls-des-menaces-80575.html

10. **Le Trésor américain s'attaque au paiement des ransomwares**
    Aux Etats-Unis, le département du Trésor a prévenu que les sociétés qui aident les entreprises victimes d'un ransomware à payer la rançon risquent des indemnités civiles.
    https://www.lemondeinformatique.fr/actualites/lire-le-tresor-americain-s-attaque-au-paiement-des-ransomwares-80577.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**.