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 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 versions antérieures à 85.0.4183.102	09/09/2020	CVE-2020-6576	85.0.4183.102 Télécharger	Mettre à jour le navigateur	-
Vulnérabilité dans Microsoft IE	De multiples vulnérabilités ont été corrigées dans Microsoft IE. Elles permettent à un attaquant de provoquer une élévation de privilèges et une exécution de code à distance. Les versions affectées sont les suivantes : • Internet Explorer 11 • Internet Explorer 9	09/09/2020	CVE-2020-1506	-	Mettre à jour via Windows Update	8.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft EDGE	De multiples vulnérabilités ont été corrigées dans Microsoft Edge. Elles permettent à un attaquant de provoquer une exécution de code à distance. Les versions affectées sont les suivantes : • Microsoft Edge (Chromium-based) • Microsoft Edge (EdgeHTML-based)	09/09/2020	CVE-2020-1172	-	Mettre à jour via Windows Update	7.5

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	Une vulnérabilité a été découverte dans le noyau Linux d'Ubuntu. Elle permet à un attaquant de provoquer une exécution de code arbitraire et un déni de service. Les systèmes affectés sont les suivants : • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS • Ubuntu 16.04 LTS • Ubuntu 14.04 ESM	09/09/2020	CVE-2020-14386	20.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://ubuntu.com/security/notices/USN-4489-1	6.7
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 une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : Google Android toutes versions sans le correctif de sécurité du 08 septembre 2020	09/09/2020	CVE-2020-0407	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité https://source.android.com/security/bulletin/2020-09-01	-

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 85.0.4183.108 (Platform version : 13310.76.0)	14/09/2020		OS85	Veuillez-vous référer au Bulletin de sécurité https://chromereleases.googleblog.com/2020/09/stable-channel-update-chrome-os_11.html	-
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, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.	14/09/2020	CVE-2020-16166	15.2	-	3.7
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été corrigées dans Microsoft Windows. Elles permettent à un attaquant de provoquer une exécution de code à distance, un contournement de la fonctionnalité de sécurité, une atteinte à la confidentialité des données, un déni de service, une élévation de privilèges et une usurpation d'identité.	09/09/2020	CVE-2020-16879	10	Mettre à jour le système via Windows Update	5.5

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Intel	De multiples vulnérabilités ont été découvertes dans les produits Intel. Elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une élévation de privilèges. Les systèmes infectés sont les suivants : • Intel AMT et Intel ISM versions antérieures à 11.8.79, 11.12.79, 11.22.79, 12.0.68 et 14.0.39 • Les processeurs Intel Core de 8ème et 9ème générations • Les processeurs Intel Core i7 de 10ème génération • Les processeurs Intel de gamme Pentium Silver • Les processeurs Intel de gammes Celeron 5000 et 4000 • Intel Driver & Support Assistant versions antérieures à 20.7.26.7	09/09/2020	CVE-2020-8758	9.17.4	Veuillez-vous référer au Bulletin de sécurité https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00404.html	9.8

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 un contournement de la fonctionnalité de sécurité.	09/09/2020	CVE-2020-1045	-	Mettre à jour le système via Windows Update	7.5
Vulnérabilité dans Microsoft Office	De multiples vulnérabilités ont été corrigées dans Microsoft Office. Elles permettent à un attaquant de provoquer une usurpation d'identité, une atteinte à la confidentialité des données, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.	09/09/2020	CVE-2020-1583	2019	Mettre à jour le système via Windows Update	5.5
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été corrigées dans les produits Microsoft. Elles permettent à un attaquant de provoquer une usurpation d'identité, une atteinte à la confidentialité des données, une élévation de privilèges, une exécution de code à distance et un contournement de la fonctionnalité de sécurité.	09/09/2020	CVE-2020-16881	-	Mettre à jour le système via Windows Update	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Nagios XI	De multiples vulnérabilités ont été découvertes dans Nagios XI. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : Nagios XI versions antérieures à 5.7.3	04/09/2020	-	5.7.3	Veuillez-vous référer au Bulletin de sécurité https://www.nagios.com/downloads/nagios-xi/change-log/	-
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, une atteinte à l'intégrité des données et une élévation de privilèges.	03/09/2020	CVE-2020-3530		Veuillez-vous référer au Bulletin de sécurité https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-UyTKCPGg	8.4

III. ACTUALITÉS

1. **Le télétravail mis en place augmente l'exposition aux cyberattaques**
   Selon une étude réalisée par AT&T, la généralisation du télétravail liée avec la crise du Covid-19 est vue comme source de failles par les RSSI.
   https://www.lemondeinformatique.fr/actualites/lire-le-teletravail-mis-en-place-augmente-l-exposition-aux-cyberattaques-80294.html

2. **L'Irlande ordonne à Facebook de ne pas envoyer de données aux US**
   La commission des données personnelles irlandaise a entamé une procédure auprès de Facebook pour invalider le transfert de données personnelles d'utilisateurs en Europe vers les Etats-Unis. Le géant des réseaux sociaux se retranche derrière les clauses contractuelles type pour poursuivre normalement ses activités.
   https://www.lemondeinformatique.fr/actualites/lire-l-irlande-ordonne-a-facebook-de-ne-pas-envoyer-de-donnees-aux-us-80332.html

3. **Faille Zerologon: un passe-partout pour l'admin dans Windows Server**
   Patchée par Microsoft en août 2020, la vulnérabilité CVE-2020-1472 surnommée Zerologon permet à un pirate de prendre le contrôle d'un domaine Windows via le protocole Netlogon. Une preuve de concept de cet exploit publié sur GitHub permet de se rendre compte de sa très grande dangerosité et de la nécessité absolue d'appliquer le correctif.
   https://www.lemondeinformatique.fr/actualites/lire-faille-zerologon-un-passe-partout-pour-l-admin-dans-windows-server-80383.html

4. **Microsoft dévoile des outils pour lutter contre les deepfakes**
   Les usurpations et tromperies consistant à manipuler grâce à l'intelligence artificielle des images aussi bien que des flux audio ou video posent de gros soucis. Pour contrecarrer l'essor des deepfakes, Microsoft a dévoilé plusieurs outils dont Video Authenticator et rejoint plusieurs initiatives dont l'AI Foundation.
   https://www.lemondeinformatique.fr/actualites/lire-microsoft-devoile-des-outils-pour-lutter-contre-les-deepfakes-80240.html

5. **Des cybercriminels chinois ciblent l'OMS et l'Europe via des campagnes de phishing sur le thème du COVID-19**
   Quel est le point commun entre le Tibet, l'OMS et les diplomates européens ? Ils sont tous dans le viseur du groupe de cybercriminels chinois APT TA413.
   https://www.undernews.fr/hacking-hacktivisme/des-cybercriminels-chinois-ciblent-loms-et-leurope-via-des-campagnes-de-phishing-sur-le-theme-du-covid-19.html

6. **Ransomware : voici les indices qui montrent que vous êtes attaqué**
   Les hackers peuvent mettre des mois à préparer des attaques de rançongiciel. Voici ce à quoi il faut faire attention si vous pensez que vous pouvez être une cible.
   https://www.zdnet.fr/pratique/ransomware-voici-les-indices-qui-montrent-que-vous-etes-attaque-39908063.htm

7. **Les cryptomonnaies servent rarement à blanchir l'argent du piratage bancaire**
   L'organisation interbancaire SWIFT vient de mettre un frein aux théories faisant des cryptomonnaies le support favori des pirates informatiques pour blanchir l'argent provenant des cyberattaques visant les groupes bancaires.
   https://www.zdnet.fr/actualites/les-cryptomonnaies-servent-rarement-a-blanchir-l-argent-du-piratage-bancaire-39909149.htm

8. **Des millions de sites WordPress piratés suite à une faille zero-day sur un plugin**
   Des millions de sites WordPress ont été victime d'attaques informatiques la semaine passée. En cause, l'exploitation par des pirates informatiques d'une faille zero-day dans un plugin de gestionnaire de fichiers.
   https://www.zdnet.fr/actualites/des-millions-de-sites-wordpress-pirates-suite-a-une-faille-zero-day-sur-un-plugin-39909231.htm

9. **Une vulnérabilité BLURtooth permet d'écraser les clés d'authentification Bluetooth**
   Tous les appareils utilisant la norme Bluetooth 4.0 à 5.0 sont vulnérables. Les correctifs ne sont pas disponibles pour l'heure.
   https://www.zdnet.fr/actualites/une-vulnerabilite-blurtooth-permet-d-ecraser-les-cles-d-authentification-bluetooth-39909441.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**.