REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse
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 2025

B.P. 6170 Tél : 694 405 868 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 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 Microsoft Edge	Une vulnérabilité a été découverte dans Microsoft Edge. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 138.0.3351.121	01/08/2025	CVE-2025-8292	138.0.3351.121 Télécharger	Mettre à jour le navigateur	8.8
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 les suivantes : • Chrome versions antérieures à 138.0.7204.183 pour Linux • Chrome versions antérieures à 138.0.7204.183/.184 pour Windows et Mac	23/07/2025	CVE-2025-8292	139.0.7258.60/.61 Télécharger	Mettre à jour le navigateur	8.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Apple Safari	De multiples vulnérabilités ont été découvertes dans Apple Safari. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Google indique que la vulnérabilité CVE-2025-6558 est activement exploitée. Les versions affectées sont les suivantes : • Safari versions antérieures à 18.6	31/07/2025	CVE-2025-6558	18.6 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 SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	01/08/2025	CVE-2025-38083	16 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-202502538-1	N/A
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 déni de service à distance, une atteinte à la confidentialité des données et un contournement de la politique de sécurité.	01/08/2025	CVE-2025-38110	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:12311	7.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Ubuntu 18.04 ESM • Ubuntu 20.04 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS • Ubuntu 25.04	01/08/2025	CVE-2025-38094	25.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7682-1	5.5

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Asterisk	De multiples vulnérabilités ont été découvertes dans Asterisk. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • asterisk versions 18.26.x antérieures à 18.26.3 • asterisk versions 20.15.x antérieures à 20.15.1 • asterisk versions 21.10.x antérieures à 21.10.1 • asterisk versions 22.5.x antérieures à 22.5.1 • asterisk versions antérieures à 20.7-cert7	01/08/2025	CVE-2025-49832	22.5.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://github.com/asterisk/asterisk/security/advisories/GHSA-v9q8-9j8m-5xwp	6.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans GLPI	De multiples vulnérabilités ont été découvertes dans GLPI. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une atteinte à l'intégrité des données et une falsification de requêtes côté serveur (SSRF). Les versions affectées sont les suivantes : • glpi versions antérieures à 10.0.19	30/07/2024	CVE-2025-53357	10.0.19 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://github.com/glpi-project/glpi/security/advisories/GHSA-x9mj-822q-6cf8	5.4
Vulnérabilité dans Python	Une vulnérabilité a été découverte dans Python. Elle permet à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • CPython sans le dernier correctif de sécurité	30/07/2025	CVE-2025-8194	3.13.5 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/ZULLF3IZ726XP5EY7XJ7YIN3K5MDYR2D/	7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Mozilla	De multiples vulnérabilités ont été découvertes dans les produits Mozilla. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Firefox ESR versions antérieures à 115.26 • Firefox ESR versions antérieures à 128.13 • Firefox ESR versions antérieures à 140.1 • Firefox versions antérieures à 141 • Firefox versions antérieures à 141 pour iOS • Thunderbird versions antérieures à 128.13 • Thunderbird versions antérieures à 140.1 • Thunderbird versions antérieures à 141	23/07/2025	CVE-2025-8044	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2025-63/	9.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Progress MOVEit	Une vulnérabilité a été découverte dans Progress MOVEit Transfer. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions affectées sont les suivantes : • MOVEit Transfer versions 2023.1.x antérieures à 2023.1.12, • MOVEit Transfer versions 2024.0.x antérieures à 2024.0.8 • MOVEit Transfer versions 2024.1.x antérieures à 2024.1.2	01/08/2025	CVE-2025-2324	17.0.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://community.progress.com/s/article/MOVEit-Transfer-Vulnerability-CVE-2025-2324-March-18-2025	8.8
Vulnérabilité dans les produits Splunk	De multiples vulnérabilités ont été découvertes dans les produits Splunk. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Enterprise Security versions antérieures à 8.1.0 • User Behavior Analytics (UBA) versions antérieures à 5.4.3	31/07/2025	CVE-2025-27144	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2025-0715	6.6

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans VMware vCenter	Une vulnérabilité a été découverte dans VMware vCenter. Elle permet à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • Cloud Foundation versions 4.5.x sans le correctif 7.0 U3v • Cloud Foundation versions 5.x sans le correctif 8.0 U3g • Telco Cloud Infrastructure versions 2.x sans le correctif de sécurité KB405542 • Telco Cloud Platform versions 2.x et 5.x sans le correctif de sécurité KB405542 • vCenter versions 7.x antérieures à 7.0 U3v • vCenter versions 8.x antérieures à 8.0 U3g	30/07/2025	CVE-2025-41241	8.0 U3g Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35964	4.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Oracle Virtualization	De multiples vulnérabilités ont été découvertes dans Oracle Virtualization. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les versions affectées sont les suivantes : • Oracle VM VirtualBox version 7.1.10	18/07/2025	CVE-2025-53030	7.1.12 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.oracle.com/security-alerts/cpujul2025.html	6.0
Vulnérabilités dans Synology BeeDrive	De multiples vulnérabilités ont été découvertes dans Synology BeeDrive. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et une atteinte à l'intégrité des données. Les versions affectées sont les suivantes : • BeeDrive versions antérieures à 1.4.2-13973 pour desktop	28/07/2025	CVE-2025-54160	1.4.2-13973 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.synology.com/fr-fr/security/advisory/Synology_SA_25_08	N/A

II.1 ACTUALITES

1. **Le bjCSIRT met OJU à la disposition des entreprises et la communauté pour une cybervigilance anticipée au Bénin**
   Jean Dans une alerte publiée le 28 juillet 2025 sur son site officiel, l'équipe béninoise de réponse aux incidents de sécurité informatique (bjCSIRT) a annoncé le développement de ***OJU***. Une plateforme open source de monitoring conçue pour la surveillance continue de la sécurité des sites des entités. Selon le bjCSIRT, ***OJU*** va permettre de répondre à un besoin de centralisation et d'automatisation de la détection des problèmes relatifs aux plateformes web où la surveillance manuelle devient rapidement inefficace. D'après les précisons de l'équipe, la fonctionnalité phare de ***OJU*** réside dans la détection automatique de défacement. Une fonctionnalité qui permet d'identifier toute altération visuelle ou textuelle suspecte d'un site web. Grâce à un système de capture et de comparaison périodique des pages, ***OJU*** signale en temps réel tout changement anormal pouvant indiquer une compromission.
   https://cybersecuritymag.africa/bjcsirt-met-oju-disposition-des-entreprises-communaute-une-cybervigilance-anticipee-au-benin

2. **Cybastion et le gouvernement ivoirien lancent la construction d'un centre de données à Abidjan**
   Abidjan entame une nouvelle ère en matière de souveraineté numérique . La première pierre du centre de données souverain de la future Cité Digitale de Côte d'Ivoire a été posée. L'annonce a été faite lundi 28 juillet 2025 par Cybastion sur sa page officielle LinkedIn. Derrière ce chantier, c'est toute une vision stratégique qui se concrétise. Celle d'un État maître de ses données et surtout capable de protéger ses infrastructures numériques et de moderniser ses services publics.
   https://cybersecuritymag.africa/cybastion-et-le-gouvernement-ivoirien-lancent-la-construction-dun-centre-de-donnees-abidjan

3. **Recrudescence des menaces cyber : la Côte d'Ivoire et le Sénégal cherchent à bâtir une sécurité numérique résiliente**
   Dans un climat régional secoué par des tensions géopolitiques et une recrudescence des menaces cyber, la Côte d'Ivoire et le Sénégal avancent leurs pions. Ce mercredi 23 juillet 2025, l'Agence Nationale de la Sécurité des Systèmes d'Information de Côte d'Ivoire (ANSSI-CI) a ouvert ses portes à une délégation du Centre des Hautes Études de Défense et de Sécurité (CHEDS) du Sénégal. À la tête de cette mission, le Général de Brigade Jean DIEME, Patron du CHEDS-Sénégal a été accompagné de dix-huit auditeurs
   https://cybersecuritymag.africa/recrudescence-des-menaces-cyber-la-cote-divoire-et-le-senegal-cherchent-batir-une-securite-numerique

4. **Escroquerie via Mobile Money : la BCLCC alerte sur une nouvelle arnaque au Burkina Faso**
   La Brigade Centrale de Lutte Contre la Cybercriminalité (BCLCC) du Burkina-Faso met en garde contre une vague d'arnaques qui cible les utilisateurs de services Mobile Money. Depuis quelques jours, plus de 60 victimes ont été recensées, avec un préjudice estimé à plus de 10 millions de francs CFA. Selon les informations communiquées par la BCLCC, cette nouvelle forme d'escroquerie repose sur une méthode bien rusée. Des individus malintentionnés, se faisant passer pour des agents des opérateurs de téléphonie mobile, appellent leurs cibles sous prétexte de procéder à une mise à jour du compte Mobile Money.
   https://cybersecuritymag.africa/la-bclcc-alerte-sur-une-nouvelle-arnaque-via-mobile-money-au-burkina-faso

5. **Linux 6.16 Released with Performance and Networking Enhancements**
   Linux creator Linus Torvalds announced the release of Linux kernel version 6.16 on July 27, 2025, marking the end of what he described as a "nice and calm" development cycle. The latest stable release brings numerous performance improvements, networking enhancements, and driver fixes across multiple hardware platforms, continuing the kernel's evolution with focused stability improvements rather than dramatic overhauls. The Linux 6.16 release represents a measured approach to kernel development, with Torvalds emphasizing the stability and predictability of this cycle.
   https://gbhackers.com/linux-6-16-released/

6. **Deepfakes en 2025 : la fraude pilotée par l'IA est déjà une réalité**
   Il n'y a pas si longtemps, les deepfakes étaient des curiosités numériques – convaincants pour certains, bancals pour d'autres, et souvent plus proches du « drôle » que de la menace. En 2025, ils sont devenus des armes cyber à part entière, disponibles commercialement et d'une dangerosité redoutable à grande échelle. Ce qui n'était au départ que de simples montages vidéo est désormais un moteur autonome au service de l'ingénierie sociale, de la fraude et du vol d'identité. Selon le rapport *AI Security Report 2025 de Check Point Research*, nous avons atteint un tournant décisif : la technologie des deepfakes s'étend désormais de la simple génération hors ligne à des moteurs d'usurpation d'identité entièrement autonomes et en temps réel, capables de tromper même les professionnels les plus aguerris.
   https://www.undernews.fr/hacking-hacktivisme/deepfakes-en-2025-la-fraude-pilotee-par-lia-est-deja-une-realite.html

III. NOTES IMPORTANTES

1. Veuillez enregistrer les adresses, alerts@cirt.cm et alerts@cirt.antic.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. CentOS 8 n'est plus supporté depuis la fin de l'année 2021. Si votre organisation n'a pas encore effectué une migration vers une version supportée notamment CentOS 8 ou 9 Stream (voir https://www.centos.org/centos-stream/) alors, votre système d'information court de grands risques. En outre, le cycle de vie des versions de CentOS 7 a été prolongé jusqu'en Juin 2024. 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.
4. Microsoft a mis fin au support de toutes les versions de Windows 7 depuis le 14 janvier 2020. Depuis cette date les systèmes fonctionnant sous Microsoft Windows 7 ne reçoivent 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 encore 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
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 l'adresses email alerts@cirt.antic.cm ou au numéro de téléphone **8202**.