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°1 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 une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 138.0.3351.65	03/07/2025	CVE-2025-49713	138.0.3351.65 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. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, un contournement de la politique de sécurité et un déni de service.	11/07/2025	CVE-2025-40014	16 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-202502264-1	7.8
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 une exécution de code arbitraire, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.	11/07/2025	CVE-2025-37799	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:10761	N/A

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. 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 versions affectées sont les suivantes : • Ubuntu 14.04 ESM • Ubuntu 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 20.04 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS • Ubuntu 24.10 • Ubuntu 25.04	11/07/2025	CVE-2025-40235	25.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/LSN-0113-1	N/A
Multiples vulnérabilités dans Microsoft Windows	De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Certaines d'entre 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.	09/07/2025	CVE-2025-49760	11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49760	3.5

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Apache HTTP Server	De multiples vulnérabilités ont été découvertes dans Apache HTTP Server. 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 atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Apache HTTP Server versions antérieures à 2.4.64	11/07/2025	CVE-2025-53020	2.4.64 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://downloads.apache.org/httpd/CHANGES_2.4.64	N/A
Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.1.x antérieures à 18.1.2	10/07/2024	CVE-2025-6948	18.1.2 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2025/07/09/patch-release-gitlab-18-1-2-released/	8.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été découvertes dans les produits Microsoft. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données.	09/07/2025	CVE-2025-49739	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49739	8.8
Vulnérabilité dans Microsoft Azure	De multiples vulnérabilités ont été découvertes dans Microsoft Azure. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Azure Monitor Agent versions antérieures à 1.35.1 • Azure Service Fabric versions antérieures à 10.1 Cumulative Update 7.0 • Microsoft SQL Server 2016 pour systèmes x64 Service Pack 3 Azure Connect Feature Pack versions antérieures à 13.0.7055.9	09/07/2025	CVE-2025-24813	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-49719	7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les Suricata	De multiples vulnérabilités ont été découvertes dans Suricata. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Suricata versions antérieures à 7.0.11	09/07/2025	CVE-2025-53538	7.0.11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://suricata.io/2025/07/08/suricata-7-0-11-released/	N/A
Vulnérabilité dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données.	09/07/2025	CVE-2025-47856	7.6.0 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-25-250	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans HPE Aruba Networking Instant On	De multiples vulnérabilités ont été découvertes dans HPE Aruba Networking Instant On. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Instant On versions antérieures à 3.2.1.0	09/07/2025	CVE-2025-37103	3.2.1.0 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworks.com/2025/hpe_aruba_networking_-_hpesbnw04894.txt	9.8
Vulnérabilités dans PHP	De multiples vulnérabilités ont été découvertes dans PHP. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, une injection SQL (SQLi) et une falsification de requêtes côté serveur (SSRF). L'éditeur a connaissance de preuves de concept pour les vulnérabilités CVE-2025-6491 et CVE-2025-1220. Les versions affectées sont les suivantes : • PHP versions 8.4.x antérieures à 8.4.10	04/07/2025	CVE-2025-6491	8.4.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.php.net/ChangeLog-8.php#8.4.10	5.9

II.1 ACTUALITES

1. **Deuxième édition des Africa CIO Tech Days (ACDT) : cybersécurité et intelligence artificielle au cœur des échanges**
   M. Jean Claude SIGUI, Président du Club des DSI-CI a lancé le jeudi 03 juillet 2025 à Abidjan, la deuxième édition des Africa CIO Tech Days (ACDT). Cette deuxième édition a été portée par le thème « Cybersécurité à l'ère de l'intelligence artificielle : combattre les cybermenaces avec des solutions innovantes ». L'initiative a été pilotée par le Club des Directeurs des Systèmes d'Information de Côte d'Ivoire (DSI-CI). Elle a rassemblé pendant deux jours des experts du digital, des décideurs technologiques et des acteurs de l'innovation, tous mobilisés pour répondre aux défis d'un continent en pleine transformation numérique.
   https://cybersecuritymag.africa/deuxieme-edition-africa-cio-tech-days-acdt-cybersecurite-et-intelligence-artificielle-au-coeur-echanges

2. **Cyber Africa Forum (CAF) 2025 : une 5e édition réussie qui place le Bénin à l'épicentre d'une nouvelle donne numérique**
   Cotonou, 26 juin 2025 – Le rideau est tombé sur la 5e édition du Cyber Africa Forum (CAF), organisée les 24 et 25 juin au Sofitel Cotonou Marina Hotel & Spa. Pendant deux jours, plus de 1000 participants dont plus de 40 décideurs publics, plus de 20 dirigeants d'agences nationales, plus de 100 leaders du secteur privé, des experts techniques, des startups disruptives et des institutions internationales se sont réunis à Cotonou, au Bénin, pour affirmer une ambition commune : placer la transformation numérique et la cybersécurité au cœur de l'agenda continental
   https://cybersecuritymag.africa/index.php/cyber-africa-forum-caf-2025-une-5-edition-reussie-qui-place-le-benin-epicentre-dune-nouvelle-donne

3. **Prochain salon africain dédié à la cyber : Niamey accueille bientôt le Handshake Digital Fair 2025**
   La capitale nigérienne s'apprête à accueillir du 24 au 26 juillet un important événement dans la sphère numérique africain. Niamey sera l'hôte du Handshake Digital Fair 2025, un salon international dédié à la cybersécurité. Ce salon est organisé par AfricaCERT en partenariat avec l'Agence Nationale de la Société de l'Information du Niger (ANSI). Cette rencontre ambitionne de rassembler les principaux acteurs du secteur : experts en cybersécurité, décideurs publics, représentants d'institutions, entreprises et chercheurs.
   https://cybersecuritymag.africa/niamey-accueille-bientot-le-handshake-digital-fair-2025

4. **Clap de fin pour le CyberDrill Régional 2025 au Congo: l'Afrique sort plus préparée face aux cybermenaces**
   Après quatre jours d'échanges, d'exercices techniques et de réflexions prospectives, la 13e édition de CyberDrill Régional s'achève aujourd'hui au Centre International de Conférences de Kintélé, en République du Congo. Lancé le 1er juillet, l'événement a rassemblé les équipes africaines de réponse aux incidents informatiques (CERTs/CIRTs) ainsi que plusieurs experts internationaux autour d'un objectif commun : renforcer la cybersécurité en Afrique. Organisé sous l'égide de l'Union Internationale des Télécommunications (UIT) et des autorités congolaises, CyberDrill Régional 2025 s'est voulu un moment clé pour faire progresser la coopération technique et institutionnelle entre les États africains face à l'ampleur des menaces cyber.
   https://cybersecuritymag.africa/clap-de-fin-pour-le-cyberdrill-regional-2025-au-congo

5. **Hackers Weaponize Compiled HTML Help to Deliver Malicious Payload**

   Threat actors have exploited Microsoft Compiled HTML Help (CHM) files to distribute malware, with a notable sample named deklaracja.chm uploaded to VirusTotal from Poland. This CHM file, a binary container for compressed HTML and associated objects, serves as a delivery vehicle for a multi-stage infection chain. Upon execution via the default hh.exe handler, the file displays a decoy image deklaracja.png, mimicking a bank transfer receipt from Polish bank PKO to lull victims while initiating malicious processes in the background.
   https://gbhackers.com/hackers-weaponize-compiled-html-help/

6. **Rapport Threat Lab WatchGuard : une augmentation de 171 % des malwares inédits détectés. Un nouveau record !**
   De Le GTIG Hausse des menaces par e-mail, multiplication des attaques furtives sur les endpoints et baisse du ransomware : un paysage façonné par l'essor de l'IA. Tribune – WatchGuard® Technologies, leader mondial de la cybersécurité unifiée à destination des fournisseurs de services managés (MSP), dévoile les résultats de son dernier rapport trimestriel sur la sécurité Internet. Ce rapport fournit une analyse approfondie des principales menaces observées sur les réseaux, les endpoints et en matière de malwares, par le WatchGuard Threat Lab au cours du 1er trimestre 2025.

   https://www.undernews.fr/malwares-virus-antivirus/rapport-threat-lab-watchguard-une-augmentation-de-171-des-malwares-inedits-detectes-un-nouveau-record.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**.