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 d'Avril 2025

B.P. 6170 Tél : 694 405 868 Web : http//www.antic.cm ; Email : infos@antic.cm

Sommaire

I. LEXIQUE DU BULLETIN 4
II. VULNÉRABILITÉS PUBLIÉES 5
II.1 NAVIGATEURS 5
Vulnérabilité dans Google Chrome 5
II.2 SYSTÈMES D'EXPLOITATION 6
Vulnérabilité dans le noyau Linux de SUSE 6
Vulnérabilité dans le noyau Linux de Debian LTS 6
Vulnérabilité dans le noyau Linux d'Ubuntu 7
Vulnérabilité dans Google Android 7
Vulnérabilité dans Microsoft Windows 8
II.3 Cms 9
Vulnérabilité dans Joomla ! 9
II.4 AUTRES 10
Vulnérabilité dans produits HPE Aruba Networking 10
Vulnérabilité dans les produits Splunk 11
Vulnérabilité dans Microsoft Azure 11
Vulnérabilités dans les GitLab 12
Vulnérabilités dans les produits Adobe 13
Vulnérabilités dans les produits Fortinet 13
Multiples vulnérabilités dans les produits Microsoft 14
II.4 ACTUALITES 15

III. NOTES IMPORTANTES 17

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 Google Chrome	Une vulnérabilité a été découverte dans Google Chrome. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Chrome versions antérieures à 135.0.7049.84/85 pour Windows et Mac • Chrome versions antérieures à 135.0.7049.84 pour Linux	09/04/2025	CVE-2025-3066	135.0.7049.84/85 Télécharger	Mettre à jour le navigateur	NA

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 exécution de code arbitraire, une élévation de privilèges et une atteinte à la confidentialité des données.	11/04/2025	CVE-2025-21888	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20251195-1	NA
Vulnérabilité dans le noyau Linux de Debian LTS	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian LTS. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Debian LTS bullseye versions antérieures à 2.0.3-9+deb11u2	11/04/2025	CVE-2023-49298	12.10.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-lts-announce/2025/04/msg00009.html	7.5

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 élévation de privilèges, un contournement de la politique de sécurité et un déni de service. Les systèmes affectés sont les suivants : • Ubuntu 14.04 ESM • Ubuntu 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 20.04 LTS • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS	11/04/2025	CVE-2025-21694	Ubuntu 24.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7429-2	5.5
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Elles permettent à un attaquant de provoquer une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Google Pixel sans les correctifs de sécurité du 10 avril 2025	11/04/2025	CVE-2025-26415	16 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2025-04-01?hl=fr	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité 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. Microsoft indique que la vulnérabilité CVE-2025-29824 est activement exploitée.	09/04/2025	CVE-2025-29824	11 Essayer	Veuillez effectuer une mise à jour via Microsoft Update	7.8

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla !	De multiples vulnérabilités ont été découvertes dans Joomla!. Elles permettent à un attaquant de provoquer une injection SQL (SQLi) et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Joomla! CMS versions 4.x antérieures à 4.4.13 • Joomla! CMS versions 5.x antérieures à 5.2.6 • Joomla! Framework versions 3.x antérieures à 3.4.0 • Joomla! Framework versions antérieures à 2.2.0	09/04/2025	CVE-2025-25227	5.2.6 Télécharger	Mettre à jour le CMS	NA

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans produits HPE Aruba Networking	De multiples vulnérabilités ont été découvertes dans les produits HPE Aruba Networking. 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 systèmes affectés sont les suivants : • AOS-10 AP versions 10.4.x antérieures à 10.4.1.6 • AOS-10 AP versions 10.7.x antérieures à 10.7.0.2 • AOS-8 Instant versions 8.10.x antérieures à 8.10.0.16 • AOS-8 Instant versions 8.12.x antérieures à 8.12.0.4 L'éditeur indique que les versions AOS-10 AP 10.6.x, AOS-10 AP 10.5.x, AOS-10 AP 10.3.x, AOS-8 Instant 8.11.x, AOS-8 Instant 8.9.x, AOS-8 Instant 8.8.x, AOS-8 Instant 8.7.x, sont affectées mais ne bénéficieront pas de correctifs de sécurité.	11/04/2025	CVE-2025-27085	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworks.com/2025/hpe_aruba_networking_-_hpesbnw04845.txt	4.9

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 : • Splunk Connect for Syslog versions antérieures à 3.34.3 • Splunk sans les derniers correctifs de sécurité • Splunk SDK for JavaScript versions antérieures à 2.0.1	10/04/2024	CVE-2024-53899	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2025-0417	8.4
Vulnérabilité dans Microsoft Azure	De multiples vulnérabilités ont été découvertes dans Microsoft Azure. Elles permettent à un attaquant de provoquer une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Azure Local Cluster versions antérieures à 2411.2 • Azure Stack HCI OS 22H2 versions antérieures à 10.0.20348.3328 • Azure Stack HCI OS 23H2 versions antérieures à 10.0.25398.1486	09/04/2025	CVE-2025-27489	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-27489	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. 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. Les versions affectées sont les suivantes : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.10.x antérieures à 17.10.4 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.9.x antérieures à 17.9.6 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions antérieures à 17.8.7	10/04/2025	CVE-2025-2469	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2025/04/09/patch-release-gitlab-17-10-4-released/	3.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Adobe	De multiples vulnérabilités ont été découvertes dans les produits Adobe. 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.	09/04/2025	CVE-2025-30294	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://helpx.adobe.com/security/products/magento/apsb25-26.html	6.5
Vulnérabilités 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.	09/04/2025	CVE-2025-25254	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-24-474	7.2

Multiples vulnérabilités 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 un déni de service à distance. Les systèmes affectés sont les suivants : • System Center Virtual Machine Manager 2022 • System Center Virtual Machine Manager 2025 • Visual Studio Code versions antérieures à 1.99.1 • Visual Studio Tools pour Applications (VSTA) 2019 versions antérieures à 16.0.35907.0 • Visual Studio Tools pour Applications (VSTA) 2022 versions antérieures à 17.0.35906.0 • VSTA 2019 SDK versions antérieures à 16.0.35907.0 • VSTA 2022 SDK versions antérieures à 17.0.35906.0	09/04/2025	CVE-2025-29821	Explorer	Veuillez effectuer une mise à jour via Microsoft Update	5.5

II.4 ACTUALITES

1. **Formation régionale en cybersécurité : Give1Project et le PNUD veulent former 150 jeunes Africains**
   Le projet Give1 en partenariat avec le Programme des Nations Unies pour le développement (PNUD) et l'université Concordia a lancé le 07 avril 2025 un appel à candidatures pour former 150 jeunes à la cybersécurité. Cette initiative entre dans le cadre de la deuxième cohorte du programme régional, après un projet pilote mené en 2023 avec 22 jeunes. L'objectif est d'élargir l'impact en accompagnant de nouveaux talents. Pour être éligible, il faut avoir entre 18 et 35 ans, être ressortissant d'un pays d'Afrique de l'Ouest ou du Centre, être inscrit ou diplômé d'un établissement supérieur, et avoir des bases en cybersécurité. Les candidats doivent aussi parler le français ou l'anglais et disposer d'une pièce d'identité valide.https://cybersecuritymag.africa/index.php/formation-regionale-en-cybersecurite-give1project-et-le-pnud-veulent-former-150-jeunes-africains

2. **Le Maroc trace la voie du futur numérique de l'Afrique lors du grand rendez-vous continental dédié à l'innovation, à l'IA et au leadership digital qui se tiendra à Marrakech**
   Le Maroc confirme une fois de plus son rôle stratégique dans l'édification du paysage numérique africain. À l'heure où le Royaume renforce sa position de hub technologique, il est également reconnu par les pays du continent comme étant une force montante clé sur la scène mondiale de la tech. C'est le message porté par les intervenants lors de la conférence de presse annuelle de GITEX AFRICA Morocco à Rabat, en amont du plus grand salon africain dédié aux technologies et aux startups, qui ouvre ses portes à Marrakech ce jour 14 au 16 avril 2025.
   https://cybersecuritymag.africa/le-maroc-trace-la-voie-du-futur-numerique-de-lafrique-au-gitex-africa-morocco-2025

3. **Immobilier en ligne : CNIN-Bénin alerte sur une arnaque sophistiquée via Whatsapp**
   Le Centre National d'Investigations Numériques du Bénin (CNIN-Bénin) a lancé mardi 08 avril 2025, une alerte sur une arnaque immobilière sophistiquée sur Whatsapp. Un stratagème redoutable qui exploite la précarité numérique et la confiance des utilisateurs. Elle cible les citoyens en quête de logement. Selon l'alerte du Centre National d'Investigations Numériques du Bénin (CNIN-Bénin), ces cyberescrocs opèrent via des groupes WhatsApp.

   https://cybersecuritymag.africa/immobilier-en-ligne-cnin-benin-alerte-sur-une-arnaque-sophistiquee-whatsapp

4. **Vers une panne totale d'Internet ? La Russie accusée de vouloir mettre le monde à genoux**
   C'est un vrai signal d'alarme que les grandes sociétés de télécommunication ont lancé. Dans un courrier adressé à l'Union européenne, au Royaume-Uni et à l'OTAN, Vodafone, Telefonica, propriétaire d'O2, et Orange préviennent qu'une hausse des attaques sur les câbles sous-marins risque de mettre en péril certains domaines essentiels. Les entreprises soulignent ainsi : « Les répercussions des dommages causés aux câbles sous-marins s'étendent bien au-delà de l'Europe, affectant potentiellement les infrastructures Internet et électriques mondiales, les communications internationales, les transactions financières et les services critiques dans le monde entier. »
   https://www.presse-citron.net/vers-une-panne-totale-dinternet-la-russie-accusee-de-vouloir-mettre-le-monde-a-genoux/

5. **Meta pourrait perdre WhatsApp et Instagram : ce scénario catastrophe devient crédible**
   C'est une affaire qui va secouer l'industrie technologique américaine. Aujourd'hui, s'ouvre un procès fatidique pour Meta outre-Atlantique. Le géant des réseaux sociaux est en effet accusé de pratiques anticoncurrentielles avec les rachats consécutifs d'Instagram et de WhatsApp, en 2012 et 2014. La plainte a initialement été déposée en 2020 par la Federal Trade Commission (FTC), organisme chargé de lutter contre les pratiques anticoncurrentielles aux États-Unis. Selon elle, Meta a acquis les deux plateformes car elle craignait leur compétitivité. Un argument corroboré par un e-mail de Mark Zuckerberg de l'époque, dans lequel il expliquait qu'il était préférable « d'acheter plutôt que de concurrencer ».
   https://www.presse-citron.net/meta-pourrait-perdre-whatsapp-et-instagram-ce-scenario-catastrophe-devient-credible/

6. **Journée mondiale de la quantique : les entreprises peuvent-elles faire face aux attaques quantiques ?**
   Malgré la puissance de l'informatique quantique, les organisations ont encore une chance réaliste de se protéger contre les attaques basées sur cette technologie, déclare Yann Samama, Senior Sales Engineer chez Gigamon. Pour cela, il est important qu'elles commencent à se préparer dès maintenant aux menaces émergentes. A l'occasion de la journée mondiale de la quantique, Yann Samama (Gigamon) révèle trois mesures qui devraient faire partie de toute stratégie de résistance au quantum. On assiste aujourd'hui à une véritable course à l'espace version XXIe siècle : des entreprises du monde entier rivalisent pour développer l'ordinateur quantique le plus puissant. Des acteurs majeurs comme les États-Unis, en particulier la Silicon Valley, le Canada, la Chine, ainsi que l'Union européenne — avec l'Allemagne et la France en tête — sont pleinement engagés dans cette compétition.
   https://www.undernews.fr/reseau-securite/journee-mondiale-de-la-quantique-les-entreprises-peuvent-elles-faire-face-aux-attaques-quantiques.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**.