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 Mai 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	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Microsoft indique que la vulnérabilité CVE-2025-4664 est activement exploitée. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 136.0.3240.76	16/05/2025	CVE-2025-4664	136.0.3240.76 Télécharger	Mettre à jour le navigateur	4.3
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. Google indique que la vulnérabilité CVE-2025-4664 est activement exploitée. Les versions affectées sont les suivantes :	15/05/2025	CVE-2025-4664	136.0.7103.113/ 114 Télécharger	Mettre à jour le navigateur	4.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• Chrome versions antérieures à 136.0.7103.113 pour Linux • Chrome versions antérieures à 136.0.7103.113/.114 pour Windows et Mac					

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 à distance, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur.	09/05/2025	CVE-2024-8805	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20251468-1	8.8
Vulnérabilité dans Google Pixel	De multiples vulnérabilités ont été découvertes dans Google Pixel. 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 le correctif du 5 mai 2025	09/05/2025	CVE-2025-27701	9 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2025-05-01?hl=fr	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 atteinte à la confidentialité des données, un contournement de la politique de sécurité et un déni de service.	09/05/2025	CVE-2025-21927	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:4509	7.8
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, une atteinte à l'intégrité des données 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 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS • Ubuntu 24.10	09/05/2025	CVE-2025-21993	Ubuntu 25.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7500-2	7.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. 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. Google indique que la vulnérabilité CVE-2025-27363 est activement exploitée.	06/05/2025	CVE-2025-27363	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2025-05-01?hl=fr	8.1
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 les vulnérabilités CVE-2025-30397, CVE-2025-30400, CVE-2025-32701, CVE-2025-32706 et CVE-2025-32709 sont activement exploitées.	14/05/2025	CVE-2025-21993	11 Télécharger	Veuillez-mettre à jour via Windows Update	7.8

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Typo3	De multiples vulnérabilités ont été découvertes dans les produits Typo3. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les versions affectées sont les suivantes : • typo3/cms-core versions 13.4.x antérieures à 13.4.12 pour composer • typo3/cms-setup versions 11.5.x antérieures à 11.5.44 pour composer • typo3/cms-setup versions 12.4.x antérieures à 12.4.31 pour composer • typo3/cms-setup versions 13.4.x antérieures à 13.4.12 pour composer • typo3/cms-webhooks versions 13.4.x antérieures à 13.4.12 pour composer	22/04/2025	CVE-2025-3647	13.4.12 Télécharger	Mettre à jour le CMS	4.3

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans produits Mozilla	De multiples vulnérabilités ont été découvertes dans les produits Mozilla. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Firefox ESR versions antérieures à 115.23.1 • Firefox ESR versions antérieures à 128.10.1 • Firefox versions antérieures à 138.0.4	19/05/2025	CVE-2025-4918	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2025-38/	7.5
Vulnérabilité dans Synology Active Backup	Une vulnérabilité a été découverte dans Synology Active Backup. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Active Backup for Microsoft 365 sans les derniers correctifs de sécurité	19/05/2024	CVE-2025-32433	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.synology.com/fr-fr/security/advisory/Synology_SA_25_06	6.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Azure	De multiples vulnérabilités ont été découvertes dans Microsoft Azure. Elles permettent à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Azure AI Document Intelligence Studio versions antérieures à 1.0.03019.1-official-7241c17a • Azure File Sync v19.0 versions antérieures à 26100 • Azure File Sync v20.0 versions antérieures à 5041884	14/05/2025	CVE-2025-30387	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30387	9.8
Vulnérabilité dans Microsoft Defender pour Endpoint	Une vulnérabilité a été découverte Microsoft Defender pour Endpoint. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Microsoft Defender pour Endpoint sur Linux versions antérieures à 101.25022.0002	16/05/2025	CVE-2025-47161	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47161	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Python	Une vulnérabilité a été découverte dans Python. Elle permet à un attaquant de provoquer un déni de service. Les versions affectées sont les suivantes : • CPython sans le dernier correctif de sécurité	16/05/2025	CVE-2025-4516	3.13.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/L75IPBBTSCYEF56I2M4KIW353BB3AY74/	5.9
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 un déni de service à distance. Fortinet indique que la vulnérabilité CVE-2025-32756 est activement exploitée.	13/04/2025	CVE-2025-32756	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-25-254	9.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits VMware	Une vulnérabilité a été découverte dans les produits VMware. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants : • Aria Automation versions 8.18.x antérieures à 8.18.1 patch 2 • Cloud Foundation versions 4.x et 5.x sans le dernier correctif de sécurité (KB394224) • Telco Cloud Platform versions 5.x sans le correctif de sécurité 8.18.1 patch 2	13/05/2025	CVE-2025-22249	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25711	8.2
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 une atteinte à la confidentialité des données.	14/05/2025	CVE-2025-32703	Explorer	Veuillez effectuer une mise à jour via Microsoft Update	5.5

II.4 ACTUALITES

1. **ISOC Bénin anime un atelier de sensibilisation sur la protection des données et la cybersécurité à Pobè**
   Internet Society-Chapitre du Bénin (ISOC Bénin) a animé ce samedi 10 mai 2025 dans la salle de conférence de l'arrondissement de Pobè dans le Département du Plateau au Bénin, un atelier de sensibilisation sur la protection de la vie privée en ligne et les enjeux de la cybersécurité. Cet atelier de sensibilisation s'inscrit dans le cadre du programme d'action 2025 de ISOC Bénin. Elle a été organisée en collaboration avec la Mairie des Jeunes de Pobè et le Cadre Concertation des Associations/Organisations de Développement (CCAD) de Pobé. L'atelier de sensibilisation a connu la présence effective du Vice-Président de l'ISOC Bénin et Consultant des TIC, M. Elias GNANCADJA. https://cybersecuritymag.africa/index.php/isoc-benin-anime-un-atelier-de-sensibilisation-sur-protection-des-donnees-cybersecurite

2. **La Somalie renforce sa cybersécurité avec un partenariat stratégique signé avec la Malaisie**
   Dans sa quête de transformation numérique, la Somalie mise sur un renforcement stratégique de la cybersécurité. Le gouvernement somalien a franchi un nouveau cap en scellant le 07 mai 2025 un protocole d'accord avec CyberSecurity Malaysia, l'Agence nationale de cybersécurité de la Malaisie. L'accord a été signé par l'Autorité nationale des communications (NCA), organe de régulation du secteur des télécoms en Somalie. Il porte sur plusieurs domaines de coopération, notamment la prévention et la gestion des incidents cybernétiques, le partage d'informations sur les menaces, le développement des compétences locales, la certification, la diplomatie cybernétique et la participation au réseau mondial Global ACE
   https://cybersecuritymag.africa/index.php/somalie-renforce-sa-cybersecurite-avec-un-partenariat-strategique-signe-avec-la-malaisie

3. **Usurpation d'identité et escroquerie en ligne : la BCLCC met fin à une série d'arnaques**
   La Brigade Centrale de Lutte Contre la Cybercriminalité (BCLCC) a interpellé quatre individus accusés d'actes d'escroquerie en ligne. Les faits reprochés concernent l'usurpation d'identité et la fraude via les technologies de l'information. Les quatre suspects, âgés de 24 à 30 ans, ont été arrêtés par la BCLCC dans le cadre de ses missions de sécurisation du cyberespace. Selon la BCLCC, les individus se présentaient comme des agents d'organisations caritatives. Par téléphone, ils passaient de fausses commandes de services traiteurs, censées être destinées à des orphelinats ou à des communautés religieuses. Ainsi, pour valider les commandes, les victimes devaient fournir une attestation de responsabilité civile.

   https://cybersecuritymag.africa/index.php/bclcc-met-fin-a-plusieurs-arnaques-en-ligne

4. **Retour sur la 1re édition du SMI-CYBER 2025 au Cameroun : les enjeux de la cybersécurité au cœur des échanges**
   La ville de Douala a abrité, du 24 au 26 avril 2025, la première édition du Salon des Métiers et des Innovations locales de Cybersécurité (SMI-CYBER). Placée sous le thème « Cyberespace africain : métiers, formation d'experts locaux et solutions endogènes de protection », cette rencontre a réuni plusieurs acteurs du numérique autour des défis liés à la cybersécurité sur le continent. Ce salon a été co-organisé par l'Association Africaine des Chercheurs en Cyberstratégie et la société RHOPEN LABS. En effet, le creuset avait pour objectif de mettre en lumière les besoins croissants en compétences en cybersécurité au Cameroun et en Afrique. Il a aussi été l'occasion de valoriser les solutions locales capables de renforcer la protection du cyberespace africain.
   https://cybersecuritymag.africa/index.php/retour-sur-la-1ere-edition-du-smi-cyber-2025-au-cameroun

5. **L'IA peut-elle vraiment tous nous mettre au chômage ? Le rêve de la Silicon Valley**
   Dans certaines sphères de la Silicon Valley, la volonté de remplacer le travail humain par des systèmes automatisés est formulée ouvertement. Nous sommes très rapidement passés de ce fantasme techno-idéologique à un objectif visé par nombre de fondateurs, d'investisseurs et de scientifiques de premier plan. Des entreprises comme Klarna se vantent de réduire leurs effectifs grâce à cette technologie, mais d'autres vont bien plus loin. C'est le cas, par exemple, de Mechanize, une start-up qui n'a même plus la décence de prétendre améliorer la productivité, puisque son projet consiste à automatiser « l'ensemble de l'économie ».
   https://www.presse-citron.net/lia-peut-mettre-chomage-reve-silicon-valley/

6. **Comprendre et prévenir les malware IA**
   Les cyberattaques trouvent souvent leur origine dans le vol d'identifiants, et les mots de passe traditionnels demeurent une vulnérabilité majeure. Leur réutilisation ou leur simplicité les rend particulièrement vulnérables, tandis que les attaques de phishing, de plus en plus sophistiquées, piègent facilement les utilisateurs, ce qui explique en partie l'explosion des fuites de données massives. Aussi, via l'obligation de la double authentification pour les entreprises et les organismes qui disposent de bases de données de plus de 2 millions de personnes, l'objectif va être de minimiser les risques d'accès non autorisés, même si les cybercriminels parviennent à obtenir des identifiants de connexion.
   https://www.undernews.fr/malwares-virus-antivirus/comprendre-et-prevenir-les-malware-ia.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**.