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 d'Avril 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 contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 136.0.3240.50	02/05/2025	CVE-2025-4096	136.0.3240.50 Télécharger	Mettre à jour le navigateur	NA
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 136.0.7103.48/49 pour Windows et Mac • Chrome versions antérieures à 136.0.7103.59 pour Linux	30/04/2025	CVE-2025-4096	136.0.7103.48/49 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 à distance, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur.	02/05/2025	CVE-2024-8805	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20251425-1	8.8
Vulnérabilité dans le noyau Linux de Debian	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Les systèmes affectés sont les suivants : • Debian bookworm versions antérieures à 6.1.135-1	02/05/2025	CVE-2025-39735	12.10.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2025/msg00069.html	7.1

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 à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Ubuntu 20.04 LTS • Ubuntu 24.04 LTS	02/05/2025	CVE-2025-2312	Ubuntu 25.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7455-5	5.9
Vulnérabilité dans le noyau Linux de Red Hat	Une vulnérabilité a été découverte dans le noyau Linux de Red Hat. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64	02/05/2025	CVE-2025-21927	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:4340	7.8

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Moodle versions 4.3.x antérieures à 4.3.12 • Moodle versions 4.4.x antérieures à 4.4.8 • Moodle versions 4.5.x antérieures à 4.5.4 • Moodle versions antérieures à 4.1.18	22/04/2025	CVE-2025-3647	5.0 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. 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. Les systèmes affectés sont les suivants : • Firefox Focus versions antérieures à 138 pour iOS • Thunderbird versions antérieures à 128.10	02/05/2025	CVE-2025-4093	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2025-32/	6.5
Vulnérabilité dans les produits Tenable	De multiples vulnérabilités ont été découvertes dans les produits Tenable. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Identity Exposure versions antérieures à 3.77.11 • Sensor Proxy version antérieures à 1.2.0	02/05/2024	CVE-2025-32433	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2025-08	10.0

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 exécution de code arbitraire à distance et une élévation de privilèges. Les systèmes affectés sont les suivants : • Azure AI Bot Service • Azure Functions • Azure Machine Learning • Azure Virtual Desktop	02/05/2025	CVE-2025-33074	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33074	7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans produits Symantec	Une vulnérabilité a été découverte dans les produits Symantec. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions affectées sont les suivantes : • Symantec Endpoint Protection versions antérieur à ERASER 119.1.7.8 • Virus and Spyware Protection definition toutes versions avant le correctif du 02 avril 2025	30/04/2025	CVE-2025-2469	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25659	6.5
Vulnérabilités dans les produits Splunk User Behavior Analytics (UBA)	De multiples vulnérabilités ont été découvertes dans les produits Splunk User Behavior Analytics (UBA). Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Splunk User Behavior Analytics (UBA) versions 5.4.x antérieures à 5.4.2	30/04/2025	CVE-2024-6345	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2025-0418	8.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits VMware	De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS) et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Tanzu Gemfire versions antérieures à 1.2.0 • Tanzu Greenplum versions antérieures à 7.4.1 • Tanzu RabbitMQ versions antérieures à 3.13.8 • Tanzu RabbitMQ versions antérieures à 4.0.3	09/04/2025	CVE-2025-30219	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25665	6.1
Multiples vulnérabilités dans les produits Microsoft	Une vulnérabilité a été découverte dans les produits Microsoft. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Dynamics 365 Customer Service	02/05/2025	CVE-2025-30391	Explorer	Veuillez effectuer une mise à jour via Microsoft Update	8.1

II.4 ACTUALITES

1. **Le Nigéria veut rejoindre le Forum mondial sur la vie privée CBPR : un pas stratégique pour la souveraineté numérique**
   À l'occasion de la prochaine conférence et assemblée annuelle du Réseau des Autorités Africaines de Protection des Données (NADPA-RAPDP), le Commissaire national de la Commission Nigériane de Protection des Données (NDPC) a tenu mercredi 30 avril 2025 une conférence adressée à la presse. Cette réunion a également été une opportunité d'annoncer l'intention du Nigéria de devenir membre associé du Global Cross-Border Privacy Rules (CBPR) Forum. Pour les autorités de la NADPA-RAPDP, la conférence et l'assemblée générale annuelle témoignent de la confiance croissante que le Nigéria gagne grâce à diverses initiatives en matière de protection des droits à la confidentialité des données.
   https://cybersecuritymag.africa/index.php/le-nigeria-veut-rejoindre-le-forum-mondial-sur-la-vie-privee-cbpr

2. **Lomé accueille la première édition du Forum International sur la Protection des Données Personnelles**
   Du 28 au 30 juillet 2025, la capitale togolaise vibrera au rythme des enjeux cruciaux de la protection des données personnelles. Le Forum International sur la Protection des Données à Caractère Personnel (FIPDCP 2025) réunira autorités de régulation, experts en cybersécurité, entreprises et société civile pour dessiner les contours d'une gouvernance numérique africaine à la fois innovante et respectueuse des droits fondamentaux. Sous l'œil avisé des spécialistes du secteur, le FIPDCP 2025 se positionne comme un cadre incontournable pour anticiper les risques cyber et harmoniser les législations. Au programme, des panels de haut niveau sur la conformité au RGPD africain (la Convention de Malabo), les innovations technologiques en matière de cryptage, et la lutte contre la cybercriminalité. La cybercriminalité, un fléau qui coûte au continent près de 4 milliards de dollars annuellement.
   https://cybersecuritymag.africa/lome-accueille-la-premiere-edition-du-forum-international-sur-la-protection-des-donnees

3. **300 collègiennes sensibilisées à la cybersécurité au Lycée Mamie Faitai en Côte d'Ivoire**
   Le Le vendredi 25 avril 2025, le Lycée de Jeunes Filles Mamie Faitai de Bingerville a accueilli une importante session de sensibilisation sur la cybersécurité. À l'initiative conjointe du Ministère de la Transition Numérique et de la Digitalisation et de l'Agence Nationale de la Sécurité des Systèmes d'Information de Côte d'Ivoire (ANSSI-CI), l'événement a réuni près de 300 élèves et encadreurs venus s'informer sur les risques numériques et les bonnes pratiques à adopter en ligne.

   https://cybersecuritymag.africa/index.php/300-collegiennes-sensibilisees-la-cybersecurite-au-lycee-mamie-faitai-en-cote-divoire

4. **L'ARPCE et l'ANSSI s'allient pour un cyberespace national souverain au Congo-Brazzaville**
   L'Agence de Régulation des Postes et des Communications Électroniques (ARPCE) et l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) de la République du Congo-Brazzaville ont officialisé ce vendredi 25 avril 2025, un protocole d'accord pour sécuriser les réseaux et le cyberespace national. Selon les autorités, cette initiative s'inscrit dans le cadre du renforcement du bouclier cybernétique de la République du Congo. Ce protocole d'accord structure une réponse concertée face à la montée des cybermenaces dans le pays. Il prévoit la mise en place de mécanismes sécurisés de partage d'informations, la coordination des actions d'urgence auprès des opérateurs télécoms ainsi qu'un renforcement mutuel des capacités techniques.
   https://cybersecuritymag.africa/index.php/arpce-et-anssi-allient-un-cyberespace-national-souverain-congo-brazzaville

5. **Les humains sont inefficaces" : Elon Musk veut remplacer les fonctionnaires par des IA**
   Il n'a pas mâché ses mots. Alors qu'il accordait un entretien avec le financier Michael Milken ce dimanche, Elon Musk a dit le fond de sa pensée concernant l'utilisation de l'intelligence artificielle pour l'action de l'administration et du gouvernement. Malheureusement, ses propos nous sont rapportés par Bloomberg, qui s'appuie sur une personne présente lors de cette conférence qui s'est tenue à huis clos dans le cadre du Milken Institute. Dès lors, nous ne disposons pas de citation exacte de l'homme d'affaires, mais cela n'en vaut pas moins le détour.
   https://www.presse-citron.net/les-humains-sont-inefficaces-elon-musk-veut-remplacer-les-fonctionnaires-par-des-ia/

6. **Rapport de la CNIL : L'authentification multi-facteur moderne, pierre angulaire de la lutte contre les cyberattaques**
   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/authentification-biometrie/rapport-de-la-cnil-lauthentification-multi-facteur-moderne-pierre-angulaire-de-la-lutte-contre-les-cyberattaques.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**.