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 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. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 137.0.3296.52	30/05/2025	CVE-2025-5283	137.0.3296.52 Télécharger	Mettre à jour le navigateur	6.5
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-2025-5419 est activement exploitée. Les versions affectées sont les suivantes : • Chrome versions antérieures à 137.0.7151.68 pour Linux • Chrome versions antérieures à 137.0.7151.68/.69 pour Windows et Mac	03/06/2025	CVE-2025-5419	137.0.7151.68/.69 Télécharger	Mettre à jour le navigateur	8.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Firefox pour iOS	Une vulnérabilité a été découverte dans Mozilla Firefox pour iOS. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Firefox versions antérieures à 139 pour iOS	22/05/2025	CVE-2025-5419	139 Télécharger	Mettre à jour le navigateur	4.3

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, une atteinte à l'intégrité des données et un contournement de la politique de sécurité.	23/05/2025	CVE-2025-39735	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-202501683-1	7.1
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 une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Les systèmes affectés sont les suivants : • Debian LTS bullseye versions antérieures à 5.10.237-1 • Debian LTS bullseye versions antérieures à 6.1.137-1~deb11u1	30/05/2025	CVE-2025-39735	12.11.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-lts-announce/2025/05/msg00045.html	7.1

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 élévation de privilèges, une atteinte à la confidentialité des données et un contournement de la politique de sécurité.	23/05/2025	CVE-2025-37749	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:8058	N/A
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans les produits Google. Elles permettent à un attaquant de provoquer une élévation de privilèges, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Android versions antérieures à 13, 14 et 15 avant le correctif du 2 juin 2025	03/06/2025	CVE-2025-27029	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2025-06-01?hl=fr	7.5

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, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Firefox ESR versions antérieures à 115.24 • Firefox ESR versions antérieures à 128.11 • Firefox versions antérieures à 139 • Thunderbird versions antérieures à 128.11 • Thunderbird versions antérieures à 139	28/05/2025	CVE-2025-5272	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2025-46/	N/A

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. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Universal Forwarder versions 9.4.x antérieures à 9.4.2 • Splunk Cloud Platform versions 9.3.2411.x antérieures à 9.3.2411.102	03/06/2024	CVE-2025-20298	Essayer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2025-0604	8.8
Vulnérabilité dans Roundcube Webmail	Une vulnérabilité a été découverte dans Roundcube Webmail. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes affectés sont les suivants : • Roundcube Webmail versions 1.5.x antérieures à 1.5.10 • Roundcube Webmail versions 1.6.x antérieures à 1.6.11	02/06/2025		1.6.11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://roundcube.net/news/2025/06/01/security-updates-1.6.11-and-1.5.10	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Apache Tomcat	Une vulnérabilité a été découverte dans Apache Tomcat. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Tomcat versions 10.1.x antérieures à 10.1.41 • Tomcat versions 11.0.x antérieures à 11.0.7 • Tomcat versions 9.0.x antérieures à 9.0.105	30/05/2025	CVE-2025-46701	11.0.7 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.7	N/A
Vulnérabilité dans Curl	De multiples vulnérabilités ont été découvertes dans Curl. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Curl versions 8.x antérieures à 8.14.0	28/05/2025	CVE-2025-5025	8.14.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://curl.se/docs/CVE-2025-5025.html	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Tenable Nessus Network Monitor	De multiples vulnérabilités ont été découvertes dans Tenable Nessus Network Monitor. 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 versions affectées sont les suivantes : • Nessus Network Monitor versions antérieures à 6.5.1	23/05/2025	CVE-2025-32415	6.5.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2025-10	7.5
Vulnérabilités dans OpenSSL	Une vulnérabilité a été découverte dans OpenSSL. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • OpenSSL versions 3.5.x antérieures à 3.5.1	23/04/2025	CVE-2025-32756	3.5.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://openssl-library.org/news/secadv/20250522.txt	N/A

II.3 ACTUALITES

1. **Cyber Africa Forum 2025 au Bénin : les inscriptions sont officiellement ouvertes**
   La 5e édition du Cyber Africa Forum se tiendra les 24 et 25 juin 2025 au Bénin à Cotonou. Les inscriptions sont officiellement lancées pour cet événement majeur dédié à la cybersécurité et à la transformation numérique en Afrique. À quelques semaines du coup d'envoi, les organisateurs du Cyber Africa Forum annoncent l'ouverture officielle des inscriptions. La prochaine édition, prévue à Cotonou, réunira plus de 1 500 participants issus des sphères publiques, privées et institutionnelles autour d'un enjeu central : la résilience de l'écosystème numérique africain. Placée sous le thème « Résilience de l'écosystème numérique : de la nécessité de changer de paradigme », cette édition 2025 ambitionne de proposer des réponses concrètes aux défis croissants de cybersécurité, d'innovation et de souveraineté numérique sur le continent
   https://cybersecuritymag.africa/index.php/cyber-africa-forum-2025-au-benin-les-inscriptions-sont-officiellement-ouvertes

2. **Le FBI arme sept (07) agents de l'ANSSI-CI pour une cyberdéfense résiliente**
   L'Agence Nationale de la Sécurité des Systèmes d'Information de Côte d'Ivoire (ANSSI-CI) a envoyé sept de ses agents du 19 au 23 mai 2025 aux États-Unis pour une formation en renforcement d'expertise en cyberdéfense au Federal Bureau of Investigation (FBI) des États-Unis. Cette initiative s'inscrit dans une tendance plus large de coopération internationale en matière de cybersécurité. Selon les experts de l'ANSSI-CI, cette collaboration souligne l'importance d'une approche coordonnée pour faire face à des menaces transnationales.
   https://cybersecuritymag.africa/index.php/fbi-arme-sept-07-agents-de-anssi-ci-pour-une-cyberdefense-resiliente

3. **L'ANSICE-Tchad lance un RN-RSSI pour assurer une cybersécurité plus résiliente des institutions du pays**
   Sous l'impulsion de l'Agence Nationale de Sécurité Informatique et de Certification Électronique du Tchad (ANSICE-Tchad) le 28 mai dernier, le pays a lancé le Réseau National des Responsables de la Sécurité des Systèmes Informatisés (RN-RSSI). Selon les autorités de l'ANSICE-Tchad, ce réseau fédère les RSSI des principales institutions publiques et privées autour d'un objectif commun. Celui d'ériger un rempart collectif face aux cybermenaces. Administration, télécommunications, finances, énergie, gouvernement…, chaque secteur critique est représenté au sein de ce réseau structuré en sections sectorielles.

   https://cybersecuritymag.africa/index.php/ansice-tchad-lance-un-rn-rssi-pour-assurer-une-cybersecurite-plus-resiliente

4. **Kaspersky dévoile que plus de 7 millions d'identifiants de comptes de streaming ont été divulgués en 2024**
   Dans son nouveau rapport, Kaspersky révèle avoir identifié plus de 7 millions de comptes compromis appartenant à des services de streaming tels que Netflix, Disney+ ou encore Amazon Prime. Pour des millions de 15-30 ans, ces plateformes de streaming jouent un rôle central dans leur socialisation et leur rapport au monde. Pour sensibiliser la Gen Z aux risques qu'ils encourent en ligne, Kaspersky lance « Case 404 », un jeu interactif sur la cybersécurité, qui leur apprend à protéger leur vie numérique. La Gen Z est friande de services de streaming, qui sont devenus un des socles de leur culture numérique. Selon des études récentes, les 15-30 ans dépensent plus sur les plateformes de streaming que n'importe quelle autre génération, mais ils sont aussi beaucoup plus actifs au sein des communautés de fans
   https://www.undernews.fr/reseau-securite/kaspersky-devoile-que-plus-de-7-millions-didentifiants-de-comptes-de-streaming-ont-ete-divulgues-en-2024.html

5. **29% des campagnes de phishing sur le cloud usurpent la marque Adobe**
   Les experts de l'organisation spécialisée dans la sécurité et les réseaux indiquent en outre qu'Adobe est la marque la plus souvent usurpée par les cybercriminels : elle apparaît en effet dans près d'un tiers (29 %) des campagnes de phishing visant à subtiliser des identifiants permettant d'accéder à des services numériques. Microsoft pointe en deuxième position avec 26 % des tentatives d'usurpation, lancées essentiellement en vue d'accéder à des comptes Microsoft 365. Ces résultats soulignent la persistance d'un cyber-risque élevé, les attaquants utilisant des méthodes d'ingénierie sociale pour exploiter la familiarité des utilisateurs européens avec les applications cloud les plus courantes en abusant de la confiance qu'ils accordent implicitement à ces outils de bureautique.
   https://www.undernews.fr/reseau-securite/phishing-hoax/29-des-campagnes-de-phishing-sur-le-cloud-usurpent-la-marque-adobe.html

6. **Gros changement sur WhatsApp : vous pourrez enfin discuter sans donner votre numéro**
   De nombreuses applications de messagerie, pour ne citer que Facebook Messenger, permettent de discuter avec une personne sans lui communiquer son numéro de téléphone. Mais WhatsApp a un fonctionnement différent, inspiré directement des SMS. Sur ce service, il est impossible d'interagir avec une autre personne sans lui communiquer votre numéro de téléphone. Cependant, WhatsApp évolue. Et visiblement, l'application s'apprête à éliminer cette contrainte qui fait partie de son ADN. Cela n'a pas encore été officialisé. Mais en fouillant dans une version beta de WhatsApp, le site WABetaInfo a découvert quelques éléments qui montrent comment cette nouveauté va fonctionner.
   https://www.presse-citron.net/gros-changement-whatsapp-discuter-sans-donner-numero/

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**.