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 Juin 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 rappelle que la vulnérabilité CVE-2025-5419 est activement exploitée. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 137.0.3296.62	04/06/2025	CVE-2025-5283	137.0.3296.62 Télécharger	Mettre à jour le navigateur	8.8
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 137.0.7151.103 pour Linux • Chrome versions antérieures à 137.0.7151.103/.104 pour Windows et Mac	11/06/2025	CVE-2025-5959	137.0.7151.103/ .104 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 exécution de code arbitraire, une élévation de privilèges et une atteinte à la confidentialité des données.	13/06/2025	CVE-2025-39735	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-202501932-1	5.5
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-2025-33053 est activement exploitée.	11/06/2025	CVE-2025-33053	11 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053	8.8

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. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un déni de service.	13/06/2025	CVE-2025-37785	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:8796	7.1

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Google	De multiples vulnérabilités ont été découvertes dans les produits Google. 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 : • Android 16 sans les correctifs du 10 juin 2025 • Pixel sans les correctifs de sécurité du 10 juin 2025	13/06/2025	CVE-2025-36887	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/android-16?hl=fr	N/A
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 : • Python for Scientific Computing versions 3.2.x antérieures à 3.2.3 • Python for Scientific Computing versions 4.2.x antérieures à 4.2.3	13/06/2024	CVE-2025-32434	Essayer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2025-0606	9.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• Splunk Machine Learning Toolkit (MLTK) versions antérieures à 5.6.0					
Vulnérabilité dans Tenable Nessus Agent	De multiples vulnérabilités ont été découvertes dans Tenable Nessus Agent. Elles permettent à un attaquant de provoquer une élévation de privilèges et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Nessus Agent versions antérieures à 10.8.5	13/06/2025	CVE-2025-36633	10.8.5 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2025-11	8.8
Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. 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 : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.10.x antérieures à 17.10.8	12/06/2025	CVE-2025-5996	17.10.8 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2025/06/11/patch-release-gitlab-18-0-2-released/	6.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.11.x antérieures à 17.11.4 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.0.x antérieures à 18.0.2					
Vulnérabilité dans les produits Microsoft	De multiples vulnérabilités ont été découvertes dans les produits Microsoft. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un contournement de la politique de sécurité.	12/06/2025	CVE-2025-47977	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47977	8.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Microsoft .Net	Une vulnérabilité a été découverte dans Microsoft .Net. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance.	12/06/2025	CVE-2025-30399	9 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-30399	7.5
Vulnérabilités dans Microsoft Office	De multiples vulnérabilités ont été découvertes dans Microsoft Office. Elles permettent à un attaquant de provoquer une exécution de code arbitraire.	12/06/2025	CVE-2025-47957	365 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-47957	8.4
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, une élévation de privilèges et un déni de service à distance.	12/06/2025	CVE-2025-32756	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://helpx.adobe.com/security/products/acrobat/apsb25-57.html	5.5

II.3 ACTUALITES

1. **Le Gabon lance une concertation nationale pour renforcer sa cybersécurité : rencontre stratégique entre ANINF - Banque Mondiale et acteurs nationaux**
   L'Agence Nationale des Infrastructures Numériques et des Fréquences du Gabon (ANINF-Gabon), la Banque Mondiale et Gabon Digital ont organisé mercredi 11 juin 2025, une rencontre autour du renforcement de la cybersécurité à Libreville. Autour de la table, le Comité technique de Gabon Digital, des Ministères, des Opérateurs privés, des Forces de l'ordre et Représentants de la société civile. Alberto Wenceslas Mounguen-gui MOUDOKI, Directeur de l'Agence Nationale des Infrastructures Numériques et des Fréquences du Gabon (ANINF-Gabon) et plusieurs autres personnalités ont pris part à cette rencontre. Elle vise amorcer un travail structurant sur le renforcement des fondations juridiques, institutionnelles et techniques de la cybersécurité au Gabon.
   https://cybersecuritymag.africa/le-gabon-lance-une-concertation-nationale-pour-renforcer-sa-cybersecurite

2. **ASIN-Bénin organise un atelier de formation en sécurité défensive à Cotonou**
   L'Agence des Systèmes d'Information et du Numérique du Bénin (ASIN-Bénin) a annoncé mardi 10 juin 2025 l'organisation d'une formation en sécurité défensive. Cette formation aura lieu à Cotonou du 17 au 20 juin 2025. Elle est ouverte à quinze participants triés sur le volet. Cette formation intensive de quatre jours, s'adresse aux néophytes comme aux professionnels souhaitant consolider leurs bases en cybersécurité défensive.
   https://cybersecuritymag.africa/asin-benin-organise-un-atelier-de-formation-en-securite-defensive-cotonou

3. **Microsoft et NC4 engagent une offensive stratégique pour la cybersécurité en Afrique**

   En marge de la deuxième Conférence Mondiale sur le Renforcement des Capacités en cybersécurité (GC3B), Microsoft a annoncé récemment le lancement d'une initiative majeure baptisée ARC (Advancing Regional Cybersecurity). Elle est destinée à renforcer la défense numérique des pays du Sud. Le premier jalon de cette offensive mondiale a été posé au Kenya. C'est avec un partenariat stratégique noué entre Microsoft et le Comité National kényan de Coordination de la cybercriminalité et de l'informatique (NC4) que les bases ont été posées.

   https://cybersecuritymag.africa/index.php/microsoft-et-nc4-engagent-offensive-cybersecurite-afrique

4. **Protection des données personnelles : ANSICE-Tchad effectue une visite guidée dans les locaux du nouveau Data Center National à N'Djamena**
   L'Agence Nationale de Sécurité Informatique et de Certification Électronique du Tchad (ANSICE-Tchad) a effectué ce mercredi 11 juin 2025 à N'Djamena, une visite guidée au nouveau Data Center National du pays. Ce nouveau Data Center a vu le jour grâce au Projet du gouvernement tchadien sur la Modernisation des Infrastructures de Communication Électronique (PMICE). Ledit projet a été appuyé par l'Agence tchadienne de Développement des Technologies et de l'Information et de la Communication (ADETIC) et Huawei Tchad. Sous la houlette de Mlle Nadjma Saleh KEBZABO, Directrice Générale Adjointe de l'ANSICE-Tchad, Directeurs techniques et Chefs de Services ont scruté chaque salle serveur et chaque baie de stockage. Il faut noter que c'est également aux côtés de M. Bobe POKA, Coordonnateur du PMICE, du Dr Zaki SABIT, Directeur des Études et de la Planification chez ADETIC et de M. BITEKE Imoma Frank Jeffrey, Directeur de projet chez Huawei Tchad que la visite a été faite.
   https://cybersecuritymag.africa/index.php/ansice-tchad-effectue-une-visite-guidee-dans-les-locaux-nouveau-data-center

5. **Kali Linux 2025.2 Released: New Tools, Smartwatch and Car Hacking Added**
   Les experts Kali Linux, the preferred distribution for security professionals, has launched its second major release of 2025, Kali Linux 2025.2, in June. This update introduces a restructured Kali Menu, upgraded desktop environments, 13 new tools, and significant Kali NetHunter advancements, including smartwatch Wi-Fi injection and a car hacking toolset. Here's a concise look at the key highlights. The most notable change in Kali 2025.2 is the revamped Kali Menu, now organized according to the MITRE ATT&CK framework.
   https://gbhackers.com/kali-linux-2025-2/

6. **Commentaires sur les cybermenaces iraniennes – Google Threat Intelligence Group**
   De Le GTIG avait publié le rapport « Tool of First Resort: Israel-Hamas War in Cyber » (L'arme de premier recours : la guerre entre Israël et le Hamas dans le cyberespace), qui contient des informations importantes sur les capacités cybernétiques pertinentes dans ce domaine. Commentaire de John Hultquist, analyste en chef, Google Threat Intelligence Group :
   » Nous nous attendons à ce que les cybercriminekls iraniens se consacrent à nouveau à des attaques contre des cibles israéliennes à la lumière des récentes actions militaires, même s'il est encore trop tôt pour en mesurer les changements. Les cyberactivités iraniennes en Israël sont déjà persistantes et agressives, et ce depuis plusieurs années
   https://www.undernews.fr/hacking-hacktivisme/commentaires-sur-les-cybermenaces-iraniennes-google-threat-intelligence-group.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**.