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 Novembre 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 142.0.3595.65	07/11/2025	CVE-2025-12727	142.0.3595.65 Télécharger	Mettre à jour le navigateur	N/A
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 142.0.7444.134 pour Linux • Chrome versions antérieures à 142.0.7444.134/.135 pour Windows • Chrome versions antérieures à 142.0.7444.135 pour Mac	06/11/2025	CVE-2025-12729	142.0.7444.134/ .135 Télécharger	Mettre à jour le navigateur	N/A

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. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	11/11/2025	CVE-2025-38664	16 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20253983-1	N/A
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 exécution de code arbitraire, un déni de service à distance et une atteinte à la confidentialité des données.	07/11/2025	CVE-2025-39849	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:19886	N/A

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 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 : • 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 25.04	07/11/2025	CVE-2025-40300	25.04.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7864-1	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Apple iOS iPadOS	De multiples vulnérabilités ont été découvertes dans Apple iOS et iPadOS. 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 systèmes affectés sont les suivants : • iOS versions antérieures à 18.7.2 • iPadOS versions antérieures à 18.7.2	06/11/2025	CVE-2025-39923	17 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.apple.com/en-us/125633	N/A
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. 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 : • Android versions antérieures à 13, 14, 15 et 16 avant le correctif du 3 novembre 2025	04/11/2025	CVE-2025-48581	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2025-11-01?hl=fr	N/A

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 atteinte à la confidentialité des données, une injection de requêtes illégitimes par rebond (CSRF) et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Moodle versions antérieures à 4.1.21 • Moodle versions antérieures à 4.4.11 • Moodle versions antérieures à 4.5.7 • Moodle versions antérieures à 5.0.3	03/11/2025	CVE-2025-62438	5.1+ Télécharger	Mettre à jour le CMS	N/A

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Suricata	De multiples vulnérabilités ont été découvertes dans Suricata. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Suricata versions 8.0.x antérieures à 8.0.2 • Suricata versions antérieures à 7.0.13	06/11/2025	CVE-2025-64344	8.0.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://suricata.io/2025/11/06/suricata-8-0-2-and-7-0-13-released/	
Vulnérabilité dans Elastic Defend	Une vulnérabilité a été découverte dans Elastic Defend. Elle permet à un attaquant de provoquer une élévation de privilèges et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Elastic Defend versions 9.x antérieures à 9.1.6 • Elastic Defend versions antérieures à 8.19.6	07/11/2025	CVE-2025-37735	9.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://discuss.elastic.co/t/elastic-defend-8-19-6-9-1-6-and-9-2-0-security-update-esa-2025-23/383272	7.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits VMware	De multiples vulnérabilités ont été découvertes dans les produits VMware. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	06/11/2025	CVE-2025-9900	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36415	8.8
Vulnérabilité dans les produits Cisco	De multiples vulnérabilités ont été découvertes dans les produits Cisco. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance. Les systèmes affectés sont les suivants : • ISE versions 3.4 antérieures à 3.4 Patch 4 • Unified CCX versions 15.x antérieures à 15.0 ES01 • Unified CCX versions antérieures à 12.5 SU3 ES07	05/11/2025	CVE-2025-20343	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-radsupress-dos-8YF3JThh	8.6

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans MISP	De multiples vulnérabilités ont été découvertes dans MISP. 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 une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • MISP versions antérieures à 2.5.24	05/11/2025		2.5.24 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.misp-project.org/security/	
Vulnérabilités dans Curl	Une vulnérabilité a été découverte dans Curl. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Curl versions 7.69.x à 8.x antérieure à 8.17.0	05/11/2025	CVE-2025-10966	8.17.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://curl.se/docs/CVE-2025-10966.html	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Dovecot	Une vulnérabilité a été découverte dans Dovecot. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Dovecot Pro core versions 2.4.x antérieures à 2.4.2	04/11/2025	CVE-2025-30189	2.4.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://documentation.open-xchange.com/dovecot/security/advisories/html/2025/oxdc-adv-2025-0001.html	7.4
Vulnérabilité dans Python	Une vulnérabilité a été découverte dans Python. Elle permet à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : • CPython sans le dernier correctif de sécurité	04/11/2024	CVE-2025-6075	3.14.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/IUP5QJ6D4KK6ULHOMPC7DPNKRYQTQNLA/	1.8

II.1 ACTUALITES

1. **Préparation à la cyberdéfense : le Cyber War Game 2025 s'achève à Dakar**
   Le Cyber War Game 2025 s'est achevé lundi ce 10 novembre 2025 à Dakar au Sénégal. Organisé par la Direction Générale du Chiffre et de la Sécurité des Systèmes d'Information du Sénégal (DCSSI-Sénégal), l'événement a réuni à Dakar des passionnés du numérique autour d'un seul défi. Celle de tester la résilience du Sénégal face aux menaces cybernétiques. L'initiative s'inscrit dans le cadre de Dakar en Jeux en prélude aux Jeux Olympiques de la Jeunesse 2026. Ce qui traduit la volonté du Sénégal de faire de la cybersécurité une priorité nationale. Au cours du Cyber War Game 2025, les équipes ont pu démontrer leurs compétences techniques, leur capacité d'analyse et leur sens du travail collaboratif face à des situations complexes.
   https://cybersecuritymag.africa/preparation-a-la-cyberdefense-le-cyber-war-game-2025-sacheve-a-dakar/

2. **L'ARTP-Sénégal et l'UCAD scellent un partenariat stratégique pour renforcer l'innovation numérique**
   L'autorité de Régulation des Télécommunications et des Postes du Sénégal (ARTP-Sénégal) et l'Université Cheikh Anta Diop (UCAD) ont signé ce mardi 11 novembre 2025, une convention de partenariat qui ouvre un nouveau chapitre dans la collaboration entre le monde académique et la régulation publique. Cette initiative vise à rapprocher la régulation des lieux de savoir pour renforcer la capacité nationale d'innovation. L'ARTP-Sénégal entend multiplier ce type de partenariat avec les universités sénégalaises afin de mieux encadrer les technologies émergentes.
   https://cybersecuritymag.africa/artp-senegal-et-ucad-scellent-un-partenariat-stratrgique-pour-renforcer-innovation-numerique/

3. **Le Libéria adopte une loi pour lutter contre la cybercriminalité**
   Le Sénat libérien a adopté le 04 novembre 2025, une loi sur la cybercriminalité. Un texte ambitieux qui marque une étape importante pour un pays encore vulnérable face aux menaces numériques. Selon ce que rapportent plusieurs médias du pays, le Sénat précise que cette loi vise à doter le Libéria d'un cadre juridique solide pour prévenir, détecter et réprimer les infractions commises dans le cyberespace. Cette loi arrive dans un contexte où les fraudes en ligne, le vol d'identité et les attaques informatiques se multiplient dans la région.
   https://cybersecuritymag.africa/le-liberia-adopte-une-loi-pour-lutter-contre-la-cybercriminalite/

4. **Transformation numérique au Soudan : un décret stratégique pour structurer données, IA et cybersécurité**
   Le Premier Ministre, Dr Kamil Idris a promulgué ce 05 novembre 2025, un décret instituant trois organismes nationaux sous la tutelle du Ministère soudanais de la Transformation Numérique et des Communications. Selon les précisions de l'autorité, cette décision s'inscrit dans la volonté du gouvernement de repenser l'appareil d'État et de renforcer son efficacité à l'ère du digital.Cette mesure constitue un pilier essentiel du Programme National de transformation numérique dans le pays. Ce nouveau décret va permettre à l'État soudanais de fournir des services plus efficaces, de protéger son cyberespace et de garantir une utilisation sûre et équitable des données et des informations. Le Soudan entend désormais maîtriser ses données, sécuriser ses infrastructures et offrir à ses citoyens des services publics modernes et fiables. Avec ce nouveau décret, le pays entend rationaliser ses institutions, harmoniser la gestion publique et surtout bâtir un système fondé sur la transparence et la souveraineté numérique.
   https://cybersecuritymag.africa/transformation-numerique-au-soudan-un-decret-strategique-pour-structurer-donnees-ia-et-cybersecurite/

5. **De puissants PC sous Android arrivent : vous aurez une bonne raison d'abandonner Windows ou macOS**
   D'après une nouvelle rumeur, Qualcomm préparerait déjà la prise en charge d'Android par ses puissantes puces Snapdragon X conçues pour les PC. Pour rappel, Google a déjà confirmé qu'il va transformer Android en système d'exploitation pour ordinateurs en combinant celui-ci avec Chrome OS. Google a déjà confirmé son intention de faire d'Android un système d'exploitation pour PC en fusionnant Android et Chrome OS. Et Qualcomm, qui est déjà l'un des principaux fournisseurs de puces pour les smartphones Android, est intéressé par cette plateforme.
   https://www.presse-citron.net/pc-sous-android-arrivent-abandonner-windows-ou-macos/

6. **Pourquoi la cybersécurité et la sobriété numérique sont indissociables dans la gestion actuelle des parcs informatiques**
   025 marque un tournant pour la gestion des actifs informatiques (ITAM). Avec l'augmentation des cyber-risques, le durcissement des réglementations et la pression croissante pour réduire les émissions, l'ITAM ne consiste plus seulement à tenir l'inventaire à jour : il s'agit désormais de mettre en place des infrastructures et des flux de travail résilients et responsables.

   https://www.undernews.fr/reseau-securite/pourquoi-la-cybersecurite-et-la-sobriete-numerique-sont-indissociables-dans-la-gestion-actuelle-des-parcs-informatiques.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**.