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 Janvier 2026

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	Une vulnérabilité a été découverte dans Microsoft Edge. Elle permet 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 144.0.3719.104	30/01/2026	CVE-2026-1504	144.0.3719.104 Télécharger	Mettre à jour le navigateur	N/A
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Firefox versions antérieures à 147.0.2	28/01/2026	CVE-2026-24869	147.0.2 Télécharger	Mettre à jour le navigateur	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome	Une vulnérabilité a été découverte dans Google Chrome. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Chrome versions antérieures à 144.0.7559.109 pour Linux • Chrome versions antérieures à 144.0.7559.109/.110 pour Windows et Mac	28/01/2026	CVE-2026-1504	144.0.7559.109/.110 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. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.	30/01/2026	CVE-2025-68766	16 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20260317-1	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 élévation de privilèges, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.	30/01/2026	CVE-2025-68305	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:1581	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 une élévation de privilèges, 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	30/01/2026	CVE-2025-39993	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7988-2	N/A

II.4 AUTRES

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. Les systèmes affectés sont les suivants : • Foundation Core pour VMware Tanzu Platform versions antérieures à 3.1.7 • Foundation Core pour VMware Tanzu Platform versions antérieures à 3.2.3 • Isolation Segmentation pour VMware Tanzu Platform versions antérieures à 10.2.7+LTS-T • Isolation Segmentation pour VMware Tanzu Platform versions antérieures à 10.3.4 • NodeJS Buildpack versions antérieures à 1.8.74 • Platform Automation Toolkit versions antérieures à 5.4.0	02/02/2026	CVE-2026-24883	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36911	3.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans ESET Inspect Connector	Une vulnérabilité a été découverte dans ESET Inspect Connector. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Inspect Connector versions antérieures à 3.0.5765 sur Windows	02/02/2026	CVE-2025-13176	3.0.5765 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support-feed.eset.com/link/15370/17266505/ca8910	8.4
Vulnérabilité dans Node.js	De multiples vulnérabilités ont été découvertes dans Node.js. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Node.js versions v20.x avec OpenSSL version 3.0.15 • Node.js versions v22.x avec OpenSSL version 3.5.4 • Node.js versions v24.x avec OpenSSL version 3.5.4 • Node.js versions v25.x avec OpenSSL version 3.5.4 L'éditeur estime que la surface d'attaque permettant d'exploiter ces vulnérabilités est faible et fournira les correctifs pour OpenSSL dans une mise à jour normale à une date ultérieure.	30/01/2026	CVE-2026-22795	25.6.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://nodejs.org/en/blog/vulnerability/openssl-fixes-in-regular-releases-jan2026	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Fortinet	Une vulnérabilité a été découverte dans les produits Fortinet. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Fortinet indique que la vulnérabilité CVE-2026-24858 est activement exploitée. Les systèmes affectés sont les suivants : • FortiAnalyzer versions 7.6.x antérieures à 7.6.6 (à venir) • FortiManager versions 7.6.x antérieures à 7.6.6 (à venir) • FortiOS versions 7.6.x antérieures à 7.6.6 (à venir) • FortiProxy versions 7.6.x antérieures à 7.6.6 (à venir) • FortiProxy versions antérieures à 7.4.13 (à venir) L'éditeur indique avoir désactivé l'authentification avec FortiCloud SSO pour les versions vulnérables. Des indicateurs de compromission sont disponibles dans l'avis éditeur.	28/01/2026	CVE-2026-24858	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-26-060	9.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Splunk Entreprise	Une vulnérabilité a été découverte dans Splunk Enterprise. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Splunk Enterprise versions 10.0.x antérieures à 10.0.3 • Splunk Enterprise versions 9.2.x antérieures à 9.2.12 • Splunk Enterprise versions 9.3.x antérieures à 9.3.9 • Splunk Enterprise versions 9.4.x antérieures à 9.4.8	30/01/2026	CVE-2025-14847	10.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2026-0101	8.7
Vulnérabilité dans OpenSSL	De multiples vulnérabilités ont été découvertes dans OpenSSL. 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 : • OpenSSL versions 3.4.x antérieures à 3.4.4 • OpenSSL versions 3.5.x antérieures à 3.5.5 • OpenSSL versions 3.6.x antérieures à 3.6.1	28/01/2026	CVE-2026-22796	3.6.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://openssl-library.org/news/secadv/20260127.txt	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Xen	De multiples vulnérabilités ont été découvertes dans Xen. Certaines d'entre 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 versions affectées sont les suivantes : • Xen version varstored master sans le correctif de sécurité xsa478.patch • Xen versions 4.18.x sans les correctifs de sécurité xsa477-4.18.patch et xsa479.patch • Xen versions 4.19.x sans le correctif de securité xsa477.patch • Xen versions xen-unstable sans les correctifs de sécurité xsa477.patch et xsa479.patch	09/01/2026	CVE-2026-23553	4.21.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://xenbits.xen.org/xsa/advisory-479.html	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Mozilla	De multiples vulnérabilités ont été découvertes dans les produits Mozilla. 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 problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Thunderbird versions antérieures à 140.7.1 • Thunderbird versions antérieures à 147.0.1	27/01/2026	CVE-2026-24869	147.0.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2026-08/	N/A
Vulnérabilité dans Python	Une vulnérabilité a été découverte dans Python. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Cpython versions antérieures à 3.15	22/01/2025	CVE-2025-12781	3.15 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/KRI7GC6S27YV5NJ4FPDALS2WI5ENAFJ6/	6.3

II.1 ACTUALITES

1. **Sensibilisation à la cybersécurité au Cameroun : le HCR et l' ANTIC outillent des réfugiés**
   L'Agence Nationale des Technologies de l'Information et de la Communication du Cameroun (ANTIC) en partenariat avec le Haut-Commissariat des Nations unies pour les réfugiés (HCR) a mené du 20 au 30 janvier 2026 une campagne de sensibilisation à la cybersécurité. Cette campagne de sensibilisation a été organisée à l'intention des réfugiés et des communautés hôtes dans les régions de l'Est, de l'Adamaoua et de l'Extrême-Nord du Cameroun. Selon l'Agence, cette initiative était destinée aux élèves et étudiants de ces communautés. Elle vise à promouvoir les bonnes pratiques en matière de cybersécurité ; à mettre en lumière les avantages des TIC pour l'éducation, la communication et les moyens de subsistance
   https://cybersecuritymag.africa/sensibilisation-a-la-cybersecurite-au-cameroun-hcr-et-antic-outillent-des-refugies/

2. **Le Gabon investit dans la formation de 1 000 jeunes talents en cybersécurité**

   Le Gabon a officiellement lancé le 27 janvier 2026, un programme de formations gratuites aux métiers du numérique et de la cybersécurité. Ledit programme nommé Africa DigiEmpower est destiné à 1 000 jeunes Gabonais. Mis en œuvre en partenariat avec la société Cybastion et l'Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF), ce projet veut renforcer les compétences des jeunes et à répondre aux besoins du marché de l'emploi.
   https://cybersecuritymag.africa/le-gabon-investit-dans-la-formation-de-1-000-jeunes-talents-en-cybersecurite/

3. **Culture de la sécurité numérique au Tchad : ANSICE organise une séance de sensibilisation des jeunes filles**
   L'Agence Nationale de Sécurité Informatique et de Certification Electronique du Tchad (ANSICE-Tchad) a organisé ce mercredi 28 janvier 2026, une session de sensibilisation à la protection des données personnelles. Cette initiative vise à renforcer la sensibilisation des jeunes filles et à promouvoir une culture de la sécurité numérique au sein de la jeunesse tchadienne. L'ANSICE-Tchad a convié les jeunes filles à cette séance à l'occasion de la Journée internationale de la protection des données personnelles. « Les jeunes filles face aux défis de la sécurisation de leurs données personnelles et de leur vie privée numérique », c'est le thème retenu pour cette édition.
   https://cybersecuritymag.africa/culture-de-la-securite-numerique-au-tchad-ansice-organise-une-seance-de-sensibilisation-des-jeunes-filles/

4. **Cybercriminalité à l'échelle mondiale : la DSC-Sénégal interpelle quatre présumés cybercriminels à Dakar**
   La Division Spéciale de Cybersécurité du Sénégal (DSC-Sénégal) a procédé ce vendredi 16 janvier 2026 à l'arrestation de quatre suspects soupçonnés d'avoir mis en place un mécanisme sophistiqué d'escroqueries en ligne à Dakar. Selon les précisions de la Division, le mécanisme comprenait manipulation de données informatiques et blanchiment de capitaux. Pendant des semaines, les enquêteurs croisent données bancaires, traces numériques, mouvements publicitaires et structures juridiques. Le travail est lent, méthodique et précis. Il débouche sur l'interpellation de quatre personnes présentées comme une cellule opérationnelle aux rôles bien répartis.
   https://cybersecuritymag.africa/cybercriminalite-a-echelle-mondiale-la-dsc-senegal-interpelle-quatre-presumes-cybercriminels-a-dakar/

5. **Protection des infrastructures critiques en Cote d'Ivoire : l'ANSSI et la EBRD annoncent le lancement d'un partenariat**
   Le DigitalHub de la European Bank for Reconstruction and Development (EBRD) et l'Agence Nationale des Systèmes de Sécurité et d'Information de Côte d'Ivoire ont annoncé le lancement d'une collaboration. Cette collaboration vise à consolider le positionnement de l'ANSSI en matière de cybersécurité et à contribuer à la protection efficace des infrastructures critiques du pays. Les autorités de EBRD ont manifesté leur enthousiasme de pouvoir accompagner l'ANSSI-Cote d'Ivoire dans ses missions et d'ouvrir la voie à de futures collaborations entre la EBRD et la Côte d'Ivoire. Une collaboration qui va permettre de promouvoir des infrastructures critiques durables et résilientes. Cette nouvelle collaboration va permettre également une affirmation en matiere de sécurité numérique en Cote d'Ivoire.
   https://cybersecuritymag.africa/protection-des-infrastructures-critiques-en-cote-ivoire-anssi-et-la-ebrd-annoncent-le-lancement-un-partenariat/

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**.