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 Février 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	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 145.0.3800.82	27/02/2026	CVE-2026-3063	145.0.3800.82 Télécharger	Mettre à jour le navigateur	8.8
Vulnérabilité dans Mozilla Firefox	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 versions affectées sont les suivantes : • Firefox versions antérieures à 148	25/02/2026	CVE-2026-2807	148 Télécharger	Mettre à jour le navigateur	9.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 144.0.7559.116 pour Linux • Chrome versions antérieures à 145.0.7632.116/117 pour Windows et Mac	24/02/2026	CVE-2026-3063	145.0.7632.116/117 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 Juniper Networks Junos OS Evolved	Une vulnérabilité a été découverte dans Juniper Networks Junos OS Evolved. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes affectés sont les suivants : • Junos OS Evolved versions antérieures à 25.4R1-S1-EVO sur PTX Series	26/02/2026	CVE-2026-21902	25.4 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://supportportal.juniper.net/s/article/2026-02-Out-of-Cycle-Security-Bulletin-Junos-OS-Evolved-PTX-Series-A-vulnerability-allows-a-unauthenticated-network-based-attacker-to-execute-code-as-root-CVE-2026-21902	9.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans HPE Aruba Networking AOS	De multiples vulnérabilités ont été découvertes dans HPE Aruba Networking AOS. 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 : • ArubaOS (AOS) versions 10.8.x antérieures à 10.8.0.1	04/03/2026	CVE-2026-23812	10.8.0.x Explorer	Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworking.hpe.com/2026/hpe_aruba_networking_-_hpesbnw05026.txt	4.3
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.	27/02/2026	CVE-2026-23089	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-202620479-1	N/A

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 un déni de service à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.	27/02/2026	CVE-2026-23074	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:3388	N/A
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 atteinte à la confidentialité des données, une atteinte à l'intégrité des données et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Ubuntu 14.04 ESM • Ubuntu 20.04 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS • Ubuntu 25.10	27/02/2026	CVE-2025-68750	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8059-6	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans le noyau Linux de Debian	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. 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. Les versions affectées sont les suivantes : • Debian trixie versions antérieures à 6.12.73-1	20/02/2026	CVE-2026-23230	13.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00050.html	N/A
Vulnérabilité dans Google Pixel	De multiples vulnérabilités ont été découvertes dans Google Pixel. 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 versions affectées sont les suivantes : • Pixel sans le correctif de sécurité du 3 mars 2026	04/03/2026	CVE-2026-0123	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2026/2026-03-01?hl=fr	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. 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. Google indique que la vulnérabilité CVE-2026-21385 est activement exploitée. Les versions affectées sont les suivantes : • Android versions antérieures à 14, 15, 16, 16-qpr2 avant le correctif du 1 mars 2026	03/03/2026	CVE-2026-21385	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2026/2026-03-01?hl=fr	7.8

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service à distance. Les systèmes affectés sont les suivants : • Wireshark versions 4.4.x antérieures à 4.4.14 • Wireshark versions 4.6.x antérieures à 4.6.4	26/02/2026	CVE-2026-3203	4.6.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.wireshark.org/security/wnpa-sec-2026-07.html	7.5
Vulnérabilité dans PostgreSQL	Une vulnérabilité a été découverte dans PostgreSQL. Elle permet à un attaquant de provoquer un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • pgvector versions antérieures à 0.8.2	26/02/2026	CVE-2026-3172	0.8.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.postgresql.org/about/news/pgvector-082-released-3245/	8.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité 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 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 ESR versions antérieures à 140.8 • Firefox pour iOS versions antérieures à 147.4 • Thunderbird versions antérieures à 148	25/02/2026	CVE-2026-2807	Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/	9.8
Vulnérabilité dans les produits Centreon	De multiples vulnérabilités ont été découvertes dans les produits Centreon. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Web versions 25.x antérieures à 25.10.9 • Open Tickets versions 25.x antérieures à 25.10.3	27/02/2026	CVE-2026-2751	25.10.9 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://thewatch.centreon.com/latest-security-bulletins-64/february-2026-monthly-security-bulletin-for-centreon-infra-monitoring-critical-5502	8.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans MISP	De multiples vulnérabilités ont été découvertes dans MISP. Certaines d'entre elles permettent à un attaquant de provoquer une falsification de requêtes côté serveur (SSRF), une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • MISP modules versions antérieures à 3.0.5 • MISP versions antérieures à 2.5.33	02/03/2026		2.5.33 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.misp-project.org/security/	
Vulnérabilité dans Tenable Nessus Manager	Une vulnérabilité a été découverte dans Tenable Nessus Manager. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Nessus Manager versions 10.11.x antérieures à 10.11.3 • Nessus Manager versions antérieures à 10.10.3	04/03/2026	CVE-2026-3493	10.11.x Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2026-08	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Microsoft	De multiples vulnérabilités ont été découvertes dans les produits Microsoft. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • azl3 erlang 26.2.5.15-1 versions antérieures à 26.2.5.17-1 • azl3 vim 9.1.1616-1 versions antérieures à 9.2.0088-1	03/03/2026	CVE-2026-28422	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-28422	2.2
Vulnérabilités dans Docker Desktop	De multiples vulnérabilités ont été découvertes dans Docker Desktop. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Docker Desktop versions antérieures à 4.62.0	03/03/2026	CVE-2026-28400	4.63.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://docs.docker.com/security/security-announcements/#docker-desktop-4620-security-update-cve-2026-28400	7.5

II.1 ACTUALITES

1. **Protection des données au Kenya : l'ODPC mise sur les médias pour promouvoir une gestion responsable des informations personnelles**
   La Commission de Protection des Données (ODPC) du Kenya a organisé ce 27 février 2026 une session de sensibilisation et d'information des médias à l'hôtel Kolel Resort. Cette session de sensibilisation a réuni des journalistes de la région d'Eldoret. Au cours de la session, les experts de la Commission ont présenté la loi de 2019 sur la Protection des Données en vigueur au Kenya. Cette sensibilisation à la protection des données aux journalistes souligne le rôle des médias dans la protection du droit à la vie privée et insiste sur l'importance d'une gestion responsable des données.
   https://cybersecuritymag.africa/odpc-mise-sur-les-medias-pour-promouvoir-une-gestion-responsable-des-informations-personnelles/

2. **Le Congo investit 39,3 millions de dollars pour accélérer sa transformation numérique**

   Le Gouvernement de la République du Congo a récemment approuvé un budget de 39,3 millions de dollars soit 21,87 milliards de francs CFA pour son Projet d'Accélération de Transformation Numérique (PATN). Pour les autorités, ce financement vise à poursuivre les efforts pour connecter le pays à l'internet à haut débit. Le Projet d'Accélération de Transformation Numérique (PATN) est un programme numérique ambitieux de la République du Congo. Il vise également à numériser les services publics et à former 1 200 jeunes aux compétences numériques.
   https://cybersecuritymag.africa/le-congo-investit-39-3-millions-de-dollars-pour-accelerer-sa-transformation-numerique/

3. **L'Algérie publie officiellement sa première Stratégie Nationale de Sécurité des Systèmes d'Information**
   L'Agence de la Sécurité des Systèmes d'Information du Ministère de la Défense Nationale de l'Algérie a publié ce mardi 03 mars 2026, la première édition de la Stratégie Nationale de Sécurité des Systèmes d'Information pour la période 2025-2029. Elle vise à garantir la cyber-résilience nationale en renforçant les capacités de prévention, de détection et de réponse aux cyberincidents, pour soutenir la transformation numérique de notre pays et préserver la souveraineté numérique nationale. ***La stratégie nationale de sécurité des systèmes d'information pour la période 2025-2029 (SNSSI 2025-2029)*** représente une feuille de route permettant la préservation de la souveraineté numérique nationale,

   https://cybersecuritymag.africa/algerie-publie-officiellement-sa-premiere-strategie-nationale-de-securite-des-systemes-information/

4. **Protection des mineurs en ligne : la Police sénégalaise et Meta posent les bases d'un partenariat opérationnel**
   Le Contrôleur Général de Police Abdoul Wahabou SALL, Directeur Général Adjoint de la Police Nationale sénégalaise a reçu le 27 février 2026 une délégation de Meta. Cette délégation était composée du Responsable des relations avec les forces de l'ordre et du chargé des politiques publiques pour l'Afrique francophone. Pendant les discussions, les échanges ont porté sur plusieurs axes de coopération prioritaires à savoir : la consolidation de la collaboration entre Meta et la Police Nationale sur des sujets de sécurité dont la protection des jeunes et des mineurs ; la présentation des dispositifs et programmes de Meta dédiés à l'appui aux forces de l'ordre. En réponse à ces directives de la Police Nationale du Sénégal, les représentants de Meta ont réaffirmé leur disponibilité à accompagner à travers des actions de renforcement de ses capacités en matière de sécurité numérique.
   https://cybersecuritymag.africa/la-police-senegalaise-et-meta-posent-les-bases-un-partenariat-operationnel/

5. **La compagnie Air Côte d'Ivoire victime d'un incident de cybersécurité**
   La compagnie aérienne nationale ivoirienne Air Côte d'Ivoire a été la cible d'une cyberattaque dans la nuit du 08 février 2026. L'attaque a entraîné une extraction illégale de données depuis son système d'information. Dans un communiqué en date du 20 février 2026, la compagnie précise avoir immédiatement enclenché ses procédures internes de gestion de crise. Les autorités compétentes ont été saisies, notamment l'Agence Nationale de la Sécurité des Systèmes d'Information de Côte d'Ivoire et l'Autorité de Régulation des Télécommunications/TIC de Côte d'Ivoire. Des investigations sont en cours avec l'appui du Côte d'Ivoire Computer Emergency Response Team et d'experts spécialisés, afin de déterminer l'origine de l'intrusion et d'évaluer l'étendue des données concernées.
   https://cybersecuritymag.africa/la-compagnie-air-cote-divoire-victime-dun-incident-de-cybersecurite/

6. **Traque aux cybercriminels au Bénin : le CNIN appréhende 56 suspects cybercriminels lors d'une vaste opération**
   Le Centre National d'Investigations Numériques (CNIN) a appréhendé ce 28 février 2026 56 cybercriminels dans plusieurs villes du Bénin. Il s'agit de Comè, de Parakou, de Porto-novo, Sèmè-Podji, Missérété, Abomey et Bohicon. Au cours de cette vaste opération, les éléments du CNIN sont intervenus simultanément dans ces différentes villes. À Comè, 19 suspects ont été arrêtés. À Parakou et dans ses environs, 14 autres ont été cueillis. Le dispositif s'est étendu à Porto-Novo, Sèmè-Podji et Missérété où 13 personnes sont tombées dans les filets des enquêteurs. À Abomey et Bohicon, 10 individus ont été appréhendés. Sur le terrain, les enquêteurs ont saisi plusieurs matériels appartenant aux cybercriminels.
   https://cybersecuritymag.africa/cnin-apprehende-56-suspects-cybercriminels-lors-une-vaste-operation/

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**.