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 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 145.0.3800.58	19/02/2026	CVE-2026-2322	145.0.3800.58 Télécharger	Mettre à jour le navigateur	N/A
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans les produits Mozilla. Elles permettent à un attaquant de provoquer 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 147.0.4	17/02/2026	CVE-2026-2447	147.0.4 Télécharger	Mettre à jour le navigateur	N/A

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 144.0.7559.109 pour Linux • Chrome versions antérieures à 145.0.7632.109/110 pour Windows et Ma	19/02/2026	CVE-2026-2650	145.0.7632.109/ 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 atteinte à la confidentialité des données, une atteinte à l'intégrité des données et un contournement de la politique de sécurité.	13/02/2026	CVE-2026-23011	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20260475-1	N/A
Vulnérabilité dans Microsoft Windows	Une vulnérabilité a été découverte dans Microsoft Windows. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Windows Admin Center versions antérieures à 2.6.4	18/02/2026	CVE-2026-26119	11 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26119	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. 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.	13/02/2026	CVE-2026-22998	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:2664	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 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 20.04 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS • Ubuntu 25.10	13/02/2026	CVE-2025-71162	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8033-4	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. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Les versions affectées sont les suivantes : • Debian bookworm versions antérieures à 6.1.162-1 • Debian trixie versions antérieures à 6.12.69-1	13/02/2026	CVE-2026-23110	13.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00036.html	N/A
Vulnérabilité dans Google Pixel	Une vulnérabilité a été découverte dans Google Pixel. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions affectées sont les suivantes : • Pixel sans le correctif de sécurité du 3 février 2026	04/02/2026	CVE-2026-0106	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2026/2026-02-01?hl=fr	N/A

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans SPIP	De multiples vulnérabilités ont été découvertes dans SPIP. 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 problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • SPIP versions 4.4.x antérieures à 4.4.9	18/02/2026		4.4.9 Télécharger	Mettre à jour le CMS	N/A
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service. Les versions affectées sont les suivantes : • Moodle versions 5.0.x antérieures à 5.0.5 • Moodle versions 5.1.x antérieures à 5.1.2 • Moodle versions antérieures à 4.5.9	17/02/2026	CVE-2026-26047	5.3 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 les produits Splunk	De multiples vulnérabilités ont été découvertes dans les produits Splunk. 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 systèmes affectés sont les suivants : • Splunk Universal Forwarder versions 10.0.x antérieures à 10.0.3 • Splunk Enterprise versions 10.0.x antérieures à 10.0.3 • Splunk Cloud Platform versions 10.0.2503 antérieures à 10.0.2503.9	19/02/2026	CVE-2026-21441	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2026-0212	8.9
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 11.0.x antérieures à 11.0.18	18/02/2026	CVE-2026-24734	11.0.18 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.52	8.4

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. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Firefox ESR versions 140.x antérieures à 140.7.1 • Firefox pour iOS versions antérieures à 147.2.1 • Thunderbird versions 147.x antérieures à 147.0.2	17/02/2026	CVE-2026-2032	Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2026-11/	N/A
Vulnérabilité dans Libre NMS	De multiples vulnérabilités ont été découvertes dans LibreNMS. Elles permettent à un attaquant de provoquer une injection SQL (SQLi) et une injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants : • LibreNMS versions antérieures à 26.2.0 • LibreNMS versions postérieures à 24.10.0 et antérieures à 26.2.0 pour composer	28/01/2026	CVE-2026-26990	26.2.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://github.com/librenms/librenms/security/advisories/GHSA-h3rv-q4rq-pqcv	8.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans PostgreSQL	De multiples vulnérabilités ont été découvertes dans PostgreSQL. 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 : • PostgreSQL versions 15.x antérieures à 15.16 • PostgreSQL versions 16.x antérieures à 16.12 • PostgreSQL versions 17.x antérieures à 17.8 • PostgreSQL versions 18.x antérieures à 18.2 • PostgreSQL versions antérieures à 14.21	13/02/2026	CVE-2026-2007	18.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.postgresql.org/about/news/postgresql-182-178-1612-1516-and-1421-released-3235/	8.2
Vulnérabilité dans Tenable Nessus Agent	Une vulnérabilité a été découverte dans Tenable Nessus Agent. Elle permet à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : • Nessus Agent versions 11.1.x antérieures à 11.1.2 • Nessus Agent versions antérieures à 11.0.4	13/02/2026	CVE-2026-2026	11.1.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2026-05	5.4

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. 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.	11/02/2026	CVE-2026-23655	4.21.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-23655	6.5
Vulnérabilités dans Microsoft Azure	De multiples vulnérabilités ont été découvertes dans Microsoft Azure. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Azure AI Language Authoring versions antérieures à 1.0.0b4 • Azure DevOps Server 2022 versions antérieures à 20260204.3 • Azure HDInsight versions antérieures à 5.1 • Azure IoT Explorer versions antérieures à 0.15.13 • Azure Local versions antérieures à 2510.0.3002	11/02/2026	CVE-2026-21531	147.0.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21531	9.8

II.1 ACTUALITES

1. **Lutte contre les préjudices en ligne : PDPO prend part à une assise régionale à Maurice**
   La Personal Data Protection Office of Uganda (PDPO) a participé du 17 au 18 février 2026 à Balaclava (Maurice) à la Réunion régionale sur le Rôle des Acteurs Étatiques dans la lutte contre les préjudices en ligne. Cette réunion a été organisée par la Collaboration on International ICT Policy for East and Southern Africa (CIPESA) en partenariat avec la Fondation Irene M. Staehelin. Elle a rassemblé des institutions nationales des droits de l'homme, des autorités de protection des données, des régulateurs des communications, des forces de l'ordre, le pouvoir judiciaire et des acteurs de la société civile de toute l'Afrique de l'Est et Australe.
   https://cybersecuritymag.africa/lutte-contre-les-prejudices-en-ligne-pdpo-prend-part-a-une-assise-regionale-a-maurice/

2. **Cybersécurité des institutions communautaires en Afrique : Google et Fondation CyberSafe lancent Resilio Africa**

   Google en partenariat avec la Fondation CyberSafe du Nigéria a lancé le 10 février 2026 Resilio Africa. Resilio Africa est une plateforme numérique pour renforcer la cybersécurité des institutions communautaires à travers l'Afrique. Elle met le cap sur des institutions de cybersécurité au Nigeria, au Kenya, au Ghana et en Afrique du Sud. Selon les précisions des initiateurs, Resilio Africa accompagnera 200 organisations (hôpitaux, écoles, médias, services d'assistance téléphonique en cas de crise et services de police). Ainsi, elle entend leur fournir des outils, des formations et un accompagnement pour améliorer leurs contrôles internes et la protection de leurs données.
   https://cybersecuritymag.africa/cybersecurite-des-institutions-communautaires-en-afrique-google-et-fondation-cybersafe-lancent-resilio-africa/

3. **Diffusion illégale de contenus intimes en ligne : le Ghana interpelle la Russie**
   Le Ghana a convoqué l'ambassadeur de Russie le mardi 17 février 2026 suite à la diffusion virale de vidéos intimes qui impliquent des femmes ghanéennes. Ces contenus ont été partagés sans le consentement des personnes filmées, ce qui a sus-cit-é une forte indignation sociale et médiatique dans le pays. La convocation a été ordonnée par le Ministère des Affaires étrangères du Ghana afin de transmettre officiellement la désapprobation du gouvernement. Les autorités du pays ont qualifié cette violation de la vie privée de « comportement atroce », contraire aux lois ghanéennes sur la protection des données et la dignité humaine.
   https://cybersecuritymag.africa/diffusion-illegale-de-contenus-intimes-en-ligne-le-ghana-interpelle-la-russie/

4. **Protection des enfants en ligne : l'UNICEF Ghana et la CSA forment les acteurs du secteur**
   La La Cyber Security Authority (CSA) en partenariat avec l'UNICEF Ghana a organisé du 12 au 13 février 2026, un programme de renforcement des capacités des acteurs de protection des enfants en ligne au Ghana. Ce programme vise à élaborer des lignes directrices sur la protection des enfants en ligne (PE) à destination des acteurs du secteur dans le pays. L'initiative permet également de lutter contre la diffusion de contenus pédopornographiques.
   https://cybersecuritymag.africa/protection-des-enfants-en-ligne-unicef-ghana-et-la-csa-forment-les-acteurs-du-secteur/

5. **Incroyable fuite de données au Sénégal : un groupe de hackers revendique 139 TB de données de la DAF sur le Dark Web**
   La Direction de l'Automatisation des Fichiers (DAF) du Sénégal a été récemment ciblée par une cyberattaque majeure. 139 TB de données de la Direction ont été mises en vente sur le Dark-Web. À l'origine de l'alerte, un message diffusé sur les réseaux sociaux et relayé par plusierus experts et médias locaux. Ces informations qui circulent, évoquent un groupe de ransomware au nom de Green Blood Group.
   https://cybersecuritymag.africa/incroyable-fuite-de-donnees-au-senegal-un-groupe-de-hackers-revendique-139-tb-de-donnees-de-la-daf-sur-le-dark-web/

6. **Google veut remplacer les photographes par cette nouvelle IA, intégrée au logiciel "Pomelli"**
   Google lance Photoshoot dans son outil Pomelli, destiné à aider les équipes marketing des PME. Photoshoot permet d'obtenir des visuels de haute qualité des produits à vendre sans recourir à un photographe professionnel. Les ingénieurs de DeepMind, le laboratoire d'IA de Google, ne cessent de développer de nouvelles idées de produits ou de fonctionnalités qui profitent des IA de la firme, comme Gemini ou Nano Banana. Et, parmi les produits qui sont actuellement testés par Google, via sa plateforme Google Labs, il y a Pomelli. Pomelli a été présenté en octobre 2025 et se présente comme un logiciel basé sur l'intelligence artificielle qui permet aux PME de générer des visuels pour leurs campagnes.
   https://www.presse-citron.net/google-remplacer-photographes-nouvelle-ia-pomelli/

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**.