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 d'Avril 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 contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Microsoft Edge pour Android versions antérieures à 147.0.3912.60 • Microsoft Edge versions antérieures à 147.0.3912.60	13/04/2026	CVE-2026-5919	147.0.3912.60 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 147.0.7727.55 pour Linux • Chrome versions antérieures à 147.0.7727.55/56 pour Windows et Mac	09/04/2026	CVE-2026-5919	147.0.7727.55/56 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 Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Elles permettent à un attaquant de provoquer un déni de service et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Android versions antérieures à 14, 15, 16 et 16-qpr2 avant le correctif du 6 avril 2026	07/04/2026	CVE-2026-0049	16 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2026/2026-04-01?hl=fr	N/A
Vulnérabilité dans le noyau Linux de SUSE	De multiples vulnérabilités ont été découvertes dans le oyau Linux de SUSE. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur.	10/04/2026	CVE-2026-23209	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20261239-1	7.8

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 une exécution de code arbitraire, une élévation de privilèges et un déni de service à distance.	10/04/2026	CVE-2026-23231	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:7100	7.8
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 une atteinte à l'intégrité des données. 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	10/04/2026	CVE-2026-23411	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8165-1	7.8

II.3 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Adobe Acrobat	Une vulnérabilité a été découverte dans Adobe Acrobat. Elle permet à un attaquant de provoquer une exécution de code arbitraire. Adobe indique que la vulnérabilité CVE-2026-34621 est activement exploitée. Les systèmes affectés sont les suivants : • Acrobat 2024 versions antérieures à 24.001.30360 sur macOS • Acrobat 2024 versions antérieures à 24.001.30362 sur Windows • Acrobat DC versions antérieures à 26.001.21411 sur Windows et macOS • Acrobat Reader DC versions antérieures à 26.001.21411 sur Windows et macOS	13/04/2026	CVE-2026-34621	**26.001.21411** Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://helpx.adobe.com/security/products/acrobat/apsb26-43.html	8.6

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Python	De multiples vulnérabilités ont été découvertes dans Python. 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 : • CPython sans les derniers correctifs de sécurité	13/04/2026	CVE-2026-3446	3.14.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/F5ZT5ICGJ6CKXVUJ34YBVY7WOZ5SHG53/	6.0
Vulnérabilité dans Foxit PDF Services API.	Une vulnérabilité a été découverte dans Foxit PDF Services API. Elle permet à un attaquant de provoquer une falsification de requêtes côté serveur (SSRF). Les systèmes affectés sont les suivants : • Foxit PDF Services API sans le dernier correctif de sécurité (aucune action utilisateur n'est requise)	13/04/2026	CVE-2026-5936	Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.foxitsoftware.com/support/security-bulletins.php	8.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité 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 systèmes affectés sont les suivants : • azl3 openssh 9.8p1-5 versions antérieures à 9.8p1-6 • azl3 openssl 3.3.5-4 versions antérieures à 3.3.5-5 • azl3 sleuthkit 4.12.1-1 versions antérieures à 4.12.1-2 • azl3 sudo 1.9.17-1 versions antérieures à 1.9.17-2 • azl3 vim 9.2.0240-1 versions antérieures à 9.2.0323-1	13/04/2026	CVE-2026-40026	4.67.0 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-28390	4.8
Vulnérabilité dans Apache TomCat	De multiples vulnérabilités ont été découvertes dans Apache Tomcat. 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 systèmes affectés sont les suivants : • Tomcat versions 11.0.x antérieures à 11.0.21	10/04/2026	CVE-2026-34500	11.0.21 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.21	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Tenable Security Center	De multiples vulnérabilités ont été découvertes dans Tenable Security Center. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Security Center versions 6.5.1, 6.6.0, 6.7.2 et 6.8.0 sans le correctif de sécurité SC202604.1	10/04/2026	CVE-2026-2006	6.8.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2026-10	8.8
Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. 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 : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.10.x antérieures à 18.10.3 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.9.x antérieures à 18.9.5	09/04/2026	CVE-2026-5173	18.9.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2026/04/08/patch-release-gitlab-18-10-3-released/	8.5

II.1 ACTUALITES

1. **La CNDP Maroc sensibilise les étudiants aux risques liés aux données personnelles**
   Une rencontre de sensibilisation a été organisée récemment à El Kelaâ des Sraghna au Maroc au profit des étudiants, autour des questions de la protection des données personnelles. Cette séance a été initiée par la Faculté des Sciences juridiques, économiques et sociales (FSJES) d'El Kelaâ des Sraghna, en partenariat avec la province et la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP). Organisée dans le cadre des efforts nationaux visant à promouvoir une culture de la cybersécurité, cette rencontre a permis de mettre en avant les défis liés à la gestion des informations personnelles à l'ère digitale. Les participants ont été sensibilisés aux risques d'atteinte à la vie privée, notamment à travers l'utilisation des réseaux sociaux, des plateformes numériques et des services en ligne.
   https://cybersecuritymag.africa/la-cndp-maroc-sensibilise-les-etudiants-aux-risques-lies-aux-donnees-personnelles/

2. **Google et l'Afrique du Sud déploient 10 000 bourses pour former la jeunesse aux métiers du numérique**
   Ce programme vise en priorité les étudiants, les enseignants et les personnels des établissements publics d'enseignement supérieur et de formation professionnelle. L'objectif est de combler le déficit de compétences digitales qui freine encore l'accès à l'emploi pour une grande partie des jeunes Sud-Africains. À travers ces bourses, les bénéficiaires pourront suivre des parcours certifiants couvrant des domaines clés comme l'analyse de données, la cybersécurité ou encore les fondamentaux de l'intelligence artificielle. Au-delà de la formation des apprenants, l'initiative prévoit également de renforcer les capacités des enseignants. Un dispositif de formation en cascade doit permettre de diffuser plus largement ces compétences au sein des institutions, avec des contenus adaptés aux réalités locales. L'ambition est d'ancrer durablement ces savoir-faire dans le système éducatif.
   https://cybersecuritymag.africa/google-et-afrique-du-sud-deploient-10-000-bourses-pour-former-la-jeunesse-aux-metiers-du-numerique/

3. **L 'ANSSI et l'ARPCE Congo renforcent la protection du cyberespace national**
   L'Agence Nationale de la Sécurité des Systèmes d'Information de (ANSSI) Congo et l' Agence de Régulation des Postes et des Communications Electroniques (ARPCE) Congo ont signé un protocole d'accord avec pour objectif le renforcement de la protection du cyberespace congolais. À travers cet accord, ANSSI et ARPCE Congo cherche à structurer une coopération durable autour de trois axes majeurs. Le premier concerne le renforcement de la sécurité des systèmes d'information et des réseaux de télécommunications, afin de mieux protéger les infrastructures critiques contre les intrusions et les attaques

informatiques. Le deuxième axe porte sur la gestion coordonnée des incidents de cybersécurité. Les deux institutions souhaitent améliorer leurs mécanismes de détection, de réaction et de traitement des incidents, afin de réduire l'impact des cyberattaques https://cybersecuritymag.africa/anssi-et-arpce-congo-renforcent-la-protection-du-cyberespace-national/

4. **La CDP-Sénégal et le Ministère de l'éducation oeuvrent pour la protection des données personnelles en milieu scolaire**
La Commission de protection des données personnelles (CDP) du Sénégal et le Ministère de l'Éducation nationale ont signé ce jeudi 09 avril 2026, une convention de partenariat pour le renforcement de l'éducation numérique et de la protection des données personnelles en milieu scolaire. Cette initiative vise à faire de chaque élève un citoyen numérique averti, capable de comprendre les implications de ses actions en ligne, de protéger ses données et de respecter celles des autres.
https://cybersecuritymag.africa/cdp-senegal-ministere-education-oeuvrent-pour-la-protection-des-donnees-personnelles/

5. **Trois présumés cybercriminels mis aux arrêts au Burkina-Faso**
Le Commissariat de Police de l'Arrondissement n°09 (CPA 09) de Ouagadougou a mis la main ce lundi 06 avril 2026 sur trois (03) individus soupçonnés d'appartenir à un réseau structuré de cybercriminalité. D'après les autorités, le groupe opérait principalement dans l'usurpation d'identité, l'escroquerie en ligne et le blanchiment de capitaux avec des méthodes rodées et difficilement traçables. Les investigations menées par les services de police révèlent un mode opératoire bien organisé. Les suspects se procuraient frauduleusement des numéros de téléphone, souvent à partir d'identités usurpées, afin de créer de faux profils sur les réseaux sociaux.
https://cybersecuritymag.africa/trois-presumes-cybercriminels-mis-aux-arrets-au-burkina-faso/

6. **Le rapport de référence sur la cyberveille à l'ère de l'IA**
Découvrez les cyberadversaires insaisissables qui amplifient leur activité grâce à l'IA et en font leur nouvelle surface d'attaque.
   - 27 secondes : le temps de propagation d'une activité cybercriminelle le plus rapide jamais enregistré
   - Augmentation de 89 % des attaques menées par des cyberadversaires qui exploitent l'IA
   - Augmentation de 42 % des vulnérabilités de type « zero day » exploitées avant qu'elles ne soient divulguées
   - 40 % des vulnérabilités exploitées par les cybercriminels associés à la Chine visant des appareils en périphérie
   - 266 % d'augmentation des intrusions commanditées par des États ciblant le cloud

https://go.crowdstrike.com/2026-global-threat-report-fr-fr.html?utm_campaign=thih&utm_content=crwd-saia-eur-fr-fr-psp-x-wht-gtr-tct_x_x_x-x-x&utm_medium=sem&utm_source=goog&utm_term=actualit%C3%A9%20cybers%C3%A9curit%C3%A9&utm_language=fr-fr&cq_cmp=23742796754&cq_plac={placement]&gad_source=1&gad_campaignid=23742796754&gclid=Cj0KCQjwy_fOBhC6ARIsAHKFB7-bo3n05PGCFmiILtp59eTRfBfryGt3g6BXtCThGUeKUbC7lrQ5WfQaAoKNEALw_wcB

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**.