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 Mars 2026

B.P. 6170 Tél : 694 405 868 Web : http//www.antic.cm ; Email : infos@antic.cm

Sommaire

I. LEXIQUE DU BULLETIN 4
II. VULNÉRABILITÉS PUBLIÉES 5
II.1 NAVIGATEURS 5
Vulnérabilité dans Microsoft Edge 5
Vulnérabilité dans Mozilla Firefox 5
Vulnérabilité dans Google Chrome 6
II.2 SYSTÈMES D'EXPLOITATION 7
Vulnérabilité dans le noyau Linux de Debian 7
Vulnérabilité dans Microsoft Windows 8
Vulnérabilité dans le noyau Linux de SUSE 8
Vulnérabilité dans le noyau Linux de Red Hat 9
Vulnérabilité dans le noyau Linux d'Ubuntu 9
Vulnérabilité dans HPE Aruba Networking AOS-CX 10
II.3 CMS 11
Vulnérabilité dans WordPress 11
II.4 AUTRES 12
Vulnérabilité dans GLPI 12
Vulnérabilité dans Curl 12
Vulnérabilité dans GitLab 13
Vulnérabilité dans les produits Apple 13
Vulnérabilité dans les produits Splunk 14

Vulnérabilité dans Python 14
Vulnérabilités dans les produits Microsoft 15
Vulnérabilités dans Microsoft Office 16
II.1 ACTUALITES 17
III. NOTES IMPORTANTES 19

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 une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Microsoft Edge pour Android versions antérieures à 145.3800.99 • Microsoft Edge pour iOS versions antérieures à 145.3800.99	13/03/2026	CVE-2026-26133	145.0.3800.99 Télécharger	Mettre à jour le navigateur	7.1
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Elles permettent à un attaquant de provoquer une exécution de code arbitraire, 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 148.0.2	11/03/2026	CVE-2026-3847	148.0.2 Télécharger	Mettre à jour le navigateur	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome	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. Google indique que les vulnérabilités CVE-2026-3909 et CVE-2026-3910 sont activement exploitées.Les versions affectées sont les suivantes : • Chrome versions antérieures à 146.0.7680.75 pour Linux • Chrome versions antérieures à 146.0.7680.75/76 pour Windows et Mac	13/03/2026	CVE-2026-3910	146.0.7680.75/76 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 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 un contournement de la politique de sécurité Les systèmes affectés sont les suivants : • Debian bookworm versions antérieures à 6.1.164-1 • Debian trixie versions antérieures à 6.12.74-2	13/03/2026	CVE-2026-23238	13 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00071.html	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance.	11/03/2026	CVE-2026-26141	11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26141	7.8
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 contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • SUSE Linux Enterprise Server 16.0 • SUSE Linux Enterprise Server for SAP Applications 16.0 • SUSE Linux Micro 6.2	13/03/2026	CVE-2025-40186	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-202620648-1	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. Elles permettent à un attaquant de provoquer une atteinte à l'intégrité des données, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur.	13/03/2026	CVE-2026-23001	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:4444	N/A
Vulnérabilité dans le noyau Linux d'Ubuntu	De multiples vulnérabilités ont été découvertes dans le noyau Linux d'Ubuntu. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS	13/03/2026	CVE-2025-37899	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8060-7	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans HPE Aruba Networking AOS-CX	De multiples vulnérabilités ont été découvertes dans HPE Aruba Networking AOS-CX. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • AOS-CX versions 10.10.x antérieures à 10.10.1180 • AOS-CX versions 10.13.x antérieures à 10.13.1161 • AOS-CX versions 10.16.x antérieures à 10.16.1030 • AOS-CX versions10.17.x antérieures à 10.17.1001	11/03/2026	CVE-2026-23817	10.17.x.x Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworking.hpe.com/2026/hpe_aruba_networking_-_hpesbnw05027.txt	6.5

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans WordPress	De multiples vulnérabilités ont été découvertes dans WordPress. 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 falsification de requêtes côté serveur (SSRF). Les versions affectées sont les suivantes : • WordPress versions antérieures à 6.9.2	11/03/2026		6.9.2 Télécharger	Mettre à jour le CMS	

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans GLPI	Une vulnérabilité a été découverte dans GLPI. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes affectés sont les suivants : • GLPI versions 11.0.x antérieures à 11.0.5	12/03/2026	CVE-2026-22248	11.0.6 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://github.com/glpi-project/glpi/security/advisories/GHSA-c9q3-mcxq-9vr4	8.0
Vulnérabilité dans Curl	De multiples vulnérabilités ont été découvertes dans Curl. 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 : • Curl versions antérieures à 8.19.0	11/03/2026	CVE-2026-3805	8.19.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://curl.se/docs/CVE-2026-3805.html	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. 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 injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 18.8.x antérieures à 18.8.6	12/02/2026	CVE-2026-3848	18.9.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2026/03/11/patch-release-gitlab-18-9-2-released/	5.0
Vulnérabilité dans les produits Apple	De multiples vulnérabilités ont été découvertes dans les produits Apple. Elles permettent à un attaquant de provoquer une exécution de code arbitraire et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • iOS versions antérieures à 15.8.7 • iOS versions antérieures à 16.7.15 • iPadOS versions antérieures à 15.8.7 • iPadOS versions antérieures à 16.7.15	12/03/2026	CVE-2024-23222	26.3.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.apple.com/en-us/126646	8.8

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 exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants : • Splunk AppDynamics Database Agent versions 26.1.x antérieures à 26.1.0 • Splunk Cloud Platform versions 10.0.2503 antérieures à 10.0.2503.12 • Splunk Enterprise versions 10.0.x antérieures à 10.0.4	12/03/2026	CVE-2026-26981	10.2.x Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2026-0313	6.5
Vulnérabilité dans Python	Une vulnérabilité a été découverte dans Python. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • CPython sans le dernier correctif de sécurité	13/03/2026	CVE-2025-13462	3.14.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/EOMI5I66ZMKQ2INNFT6T7IAIKUGPZYIE/	2.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Microsoft	Une vulnérabilité a été découverte dans les produits Microsoft. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Microsoft Loop pour iOS versions antérieures à 2.106.26020617 • Microsoft PowerBI pour Android versions antérieures à 2.2.260210.21290750 • Microsoft PowerBI pour iOS versions antérieures à 1.2.260302.2193910 • Microsoft Teams pour Android versions antérieures à 1.0.0.2026043102 • Microsoft Teams pour iOS versions antérieures à 8.3.1	13/03/2026	CVE-2026-26133	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26133	7.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Microsoft Office	Une vulnérabilité a été découverte dans Microsoft Office. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données.	13/03/2026	CVE-2026-26133	365 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26133	7.1

II.1 ACTUALITES

1. **Usurpation d'identité et cyberescroquerie au Burkina-Faso : la Police nationale intercepte trois présumés cybercriminels**
   Au Burkina Faso, trois individus suspectés d'activités de cyber-escroquerie ont été arrêtés par la Police nationale. Les mis en cause sont présentés comme des présumés auteurs d'usurpation d'identité sur les plates-formes numériques et d'escroquerie via système électronique. Ces pratiques consistent à manipuler les victimes, notamment par des échanges en ligne, pour les amener à divulguer des informations sensibles ou à effectuer des paiements. Les trois suspects ont été placés à la disposition des services compétents pour la suite de la procédure judiciaire.
   https://cybersecuritymag.africa/usurpation-didentite-et-cyberescroquerie-au-burkina-faso-la-police-nationale-intercepte-trois-presumes-cybercriminels/

2. **Sensibilisation aux cyber-risques en Egypte : le pays lance une plateforme éducative**
   Dans le cadre de cette initiative, le Ministère a lancé une nouvelle plateforme en ligne Wa3i.net. Elle est conçue comme un centre de connaissances communautaire qui offre un contenu spécialisé en langue arabe adapté aux groupes cibles. Par ailleurs, Wa3i.net propose des ressources pour les enfants, les adolescents, les enseignants et les parents en les aidant à mieux comprendre l'utilisation responsable des technologies et les pratiques en ligne sécurisées. La plateforme se veut un centre de connaissances dédié à la sécurité numérique. Accessible en langue arabe, elle propose des contenus pédagogiques, des guides pratiques et des ressources éducatives destinés à différents publics, notamment les enfants, les adolescents, les parents et les enseignants.
   https://cybersecuritymag.africa/sensibilisation-aux-cyber-risques-en-egypte-le-pays-lance-une-plateforme-educative/

3. **Le Ghana signe un mémorandum avec la Corée du Sud pour accélérer sa transformation numérique**
   Le Ghana et la Corée du Sud ont renforcé leur partenariat en signant un mémorandum dans le domaine des technologies numériques. Cette orientation a été confirmée lors d'une rencontre bilatérale tenue le 11 mars 2026 à Séoul, au cours de laquelle les deux pays ont convenu d'élargir leur partenariat à l'innovation technologique et à la transformation numérique. Les deux dirigeants ont également mis en avant les perspectives offertes par le développement des technologies et de l'innovation pour soutenir la croissance économique et renforcer les relations bilatérales.
   https://cybersecuritymag.africa/le-ghana-signe-un-memorandum-avec-la-coree-du-sud-pour-accelerer-sa-transformation-numerique/

4. **La Somalie inaugure son premier centre national de réponse aux incidents cyber**
   Le gouvernement a officiellement inauguré le samadi 7 mars 2026 le Somalia Computer Incident Response Team (SOMCIRT). Il s'agit du premier centre national dédié à la gestion et à la coordination des incidents de cybersécurité en Somalie. Placé sous la supervision de la National Communications Authority (NCA), il aura pour mission de surveiller les menaces numériques, d'analyser les incidents de sécurité et de coordonner les actions de réponse lorsqu'une attaque est détectée. Le dispositif doit également permettre d'améliorer la coopération entre les institutions publiques, les opérateurs télécoms et les entreprises technologiques. En centralisant les informations relatives aux incidents cyber, le SOMCIRT pourra diffuser des alertes, partager des recommandations de sécurité et soutenir les organisations confrontées à des attaques.
   https://cybersecuritymag.africa/la-somalie-inaugure-son-premier-centre-national-de-reponse-aux-incidents-cyber/

5. **Impossible de stopper le shadow AI : voici comment en faire une force**
   Les directions informatiques connaissent bien le phénomène du shadow IT : ces logiciels ou services utilisés par les collaborateurs sans validation officielle. Pendant des années, les entreprises ont tenté d'y répondre par des politiques de contrôle ou de blocage. Mais l'intelligence artificielle change profondément la donne. Contrairement aux applications SaaS traditionnelles, les outils d'IA générative ne nécessitent aucune installation. Ils sont accessibles instantanément depuis un navigateur ou un smartphone. En quelques secondes, un collaborateur peut demander à une IA de résumer un document, générer un texte, analyser des données ou produire du code.
   https://www.undernews.fr/undernews/impossible-de-stopper-le-shadow-ai-voici-comment-en-faire-une-force.html

6. **Google Warns of AI-Driven Adaptive Malware That Rewrites Its Own Code To Evade Detection**
   In a groundbreaking report, Google's cybersecurity arm, Mandiant, has raised the alarm about the rising threat of AI-driven, adaptive malware. This type of malware can change its code on the fly, evading traditional security systems. As cybercriminals adopt sophisticated techniques powered by artificial intelligence (AI), the threat landscape is evolving at an alarming rate. Adaptive malware is malicious software that modifies its behavior or appearance based on the environment it encounters. Using AI, this malware can analyze the security systems it faces and rewrite its own code to bypass detection.
   https://cyberpress.org/ai-malware-rewrites-code/

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**.