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 Mars 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 146.0.3856.84	31/03/2026	CVE-2026-4678	145.0.3856.84 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. Google indique que la vulnérabilité CVE-2026-5281 est activement exploitée. Les versions affectées sont les suivantes : • Chrome versions antérieures à 146.0.7680.177 pour Linux • Chrome versions antérieures à 146.0.7680.177 pour Windows • Chrome versions antérieures à 146.0.7680.178 pour Mac	01/04/2026	CVE-2026-5292	146.0.7680.177 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 Cisco IOS et IOS XE	De multiples vulnérabilités ont été découvertes dans Cisco IOS et IOS XE. Elles permettent à un attaquant de provoquer un déni de service à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • IOS XE, se référer au bulletin de sécurité de l'éditeur pour les versions vulnérables. • IOS, se référer au bulletin de sécurité de l'éditeur pour les versions vulnérables	26/03/2026	CVE-2026-20125	17.15.x Explorer	Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-secureboot-bypass-B6uYxYSZ	7.5
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.	27/03/2026	CVE-2026-25702	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20261089-1	9.8

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 une atteinte à la confidentialité des données.	27/03/2026	CVE-2026-23001	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : ttps://access.redhat.com/errata/RHSA-2026:5821	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 exécution de code arbitraire, une élévation de privilèges et une atteinte à la confidentialité des données. 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 • Ubuntu 25.10	27/03/2026	CVE-2026-29111	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8098-9	5.5

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla !	De multiples vulnérabilités ont été découvertes dans Joomla!. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à l'intégrité des données, une injection SQL (SQLi) et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Joomla! versions 6.x antérieures à 6.0.4 • Joomla! versions antérieures à 5.4.4	01/04/2026	CVE-2026-23899	6..0.4 Télécharger	Mettre à jour le CMS	8.6

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans ISC BIND	De multiples vulnérabilités ont été découvertes dans ISC BIND. 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 : • BIND Supported Preview Edition versions 9.20.x antérieures à 9.20.21-S1 • BIND versions 9.21.x antérieures à 9.21.20	26/03/2026	CVE-2026-3591	9.21.20 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://kb.isc.org/v1/docs/cve-2026-3591	5.4
Vulnérabilité dans Grafana	De multiples vulnérabilités ont été découvertes dans Grafana. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance. Les systèmes affectés sont les suivants : • Grafana versions 12.4.x antérieures à 12.4.2	26/03/2026	CVE-2026-27880	12.4.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://grafana.com/blog/grafana-security-release-critical-and-high-severity-security-fixes-for-cve-2026-27876-and-cve-2026-27880/	7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Zabbix	De multiples vulnérabilités ont été découvertes dans Zabbix. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Zabbix versions 7.0.22 sans le dernier correctif de sécurité	27/03/2026	CVE-2025-66578	7.4.9rc Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.zabbix.com/browse/ZBX-27458	7.5
Vulnérabilité dans Docker Desktop	Une vulnérabilité a été découverte dans Docker Desktop. Elle permet à un attaquant de provoquer une falsification de requêtes côté serveur (SSRF). Les systèmes affectés sont les suivants : • Docker Desktop versions antérieures à 4.67.0	30/03/2026	CVE-2026-33990	4.67.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://docs.docker.com/security/security-announcements/#docker-desktop-4670-security-update-cve-2026-33990	6.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Roundcube	Une vulnérabilité a été découverte dans Roundcube. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Roundcube Webmail versions 1.5.x antérieures à 1.5.15 • Roundcube Webmail versions 1.6.x antérieures à 1.6.15 • Roundcube Webmail versions 1.7.x antérieures à 1.7-rc6	30/03/2026		1.7-rc6 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://roundcube.net/news/2026/03/29/security-updates-1.7-rc6-1.6.15-1.5.15	
Vulnérabilité dans Symantec Data Loss Prevention (DLP)	Une vulnérabilité a été découverte dans Symantec Data Loss Prevention (DLP). Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Data Loss Prevention (DLP) versions antérieures à 16.0 MP2 HF15 (16.0.00215.62094) • Data Loss Prevention (DLP) versions antérieures à 16.0 RU1 MP1 HF12 (16.0.10112.60928) • Data Loss Prevention (DLP) versions antérieures à 16.0 RU2 HF9 (16.0.20009.60689) • Data Loss Prevention (DLP) versions antérieures à 16.1 MP2	31/03/2026	CVE-2026-3991	16.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37306	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	(16.1.00200.60431) • Data Loss Prevention (DLP) versions antérieures à 25.1 MP1 (25.1.00100.60229)					
Vulnérabilité dans les produits FoxIT	De multiples vulnérabilités ont été découvertes dans les produits FoxIT. 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. Les systèmes affectés sont les suivants : • PDF Editor pour Mac versions 14.x antérieures à 14.0.3 • PDF Editor pour Mac versions antérieures à 2026.1 • PDF Editor versions 14.x antérieures à 14.0.3 • PDF Editor versions antérieures à 2026.1 • PDF Reader pour Mac versions antérieures à 2026.1 • PDF Reader versions antérieures à 2026.1	31/03/2026	CVE-2026-3780	Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.foxitsoftware.com/support/security-bulletins.php	7.3

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 bind 9.20.18-1 versions antérieures à 9.20.21-1 • azl3 flannel 0.24.2-26 versions antérieures à 0.24.2-26 • azl3 libssh 0.10.6-6 versions antérieures à 0.10.6-6 • azl3 ocaml 5.1.1-2 versions antérieures à 5.1.1-2 • azl3 telegraf 1.31.0-17 versions antérieures à 1.31.0-17 • azl3 trident 0.21.0-1 versions antérieures à 0.22.0-1 • cbl2 nodejs18 18.20.3-12 versions antérieures à 18.20.3-12 • cbl2 ocaml 4.13.1-3 versions antérieures à 4.13.1-3 • cbl2 systemd-bootstrap 250.3-14 versions antérieures à 250.3-14 • cbl2 telegraf 1.29.4-22 versions antérieures à 1.29.4-22	01/04/2026	CVE-2026-34353	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34353	5.9

II.1 ACTUALITES

1. **L'ANSICE Tchad sensibilise les élèves au cyberharcèlement**
   L'Agence Nationale de Sécurité Informatique et de Certification Électronique (ANSICE) Tchad a animé du 24 au 31 mars 2026 une série de sessions de sensibilisation au cyberharcèlement et aux bonnes pratiques numériques. Cette initiative de l'institution a pour objectif d'outiller les élèves du Lycée Français Montaigne de N'Djamena. Pendant une semaine, les élèves et encadreurs ont été outillés face aux risques du cyberespace et aux comportements responsables à adopter en ligne. Par ailleurs, les élèves ont été confrontés à la portée réelle de leurs usages numériques, à la violence parfois invisible des interactions en ligne et à la responsabilité individuelle qui accompagne chaque publication.
   https://cybersecuritymag.africa/ansice-tchad-sensibilise-les-eleves-au-cyberharcelement/

2. **KNext 2026 à Abidjan : Kaspersky alerte sur la recrudescence des cyberattaques en Afrique de l'Ouest**
   Le 25 mars 2026, Kaspersky a organisé au Sofitel Abidjan Hôtel Ivoire une conférence consacrée à la cybersécurité, réunissant ses experts et des professionnels IT ivoiriens pour analyser l'évolution des menaces numériques en Afrique de l'Ouest. Cette rencontre, organisée dans le cadre de l'événement KNext, visait à alerter sur l'intensification des cyberattaques et à proposer des réponses adaptées face à des risques financiers et stratégiques croissants. Lors de ce creuset les spécialistes ont dressé un constat préoccupant. En effet, des opérations d'envergure à l'image de PassiveNeuron, ont démontré la capacité d'attaquants à infiltrer des infrastructures critiques. Entre fin 2024 et mi-2025, cette campagne de cyberespionnage a compromis des serveurs SQL d'organisations clés grâce à des implants sophistiqués, confirmant un changement d'échelle et de complexité des attaques visant le continent.
   https://cybersecuritymag.africa/knext-2026-a-abidjan-kaspersky-alerte-sur-la-recrudescence-des-cyberattaques-en-afrique-de-louest/

3. **Cybersécurité des PME en Ouganda : vers une norme adaptée pour soutenir la transformation numérique**
   L'Autorité nationale des technologies de l'information (NITA-U) de l'Ouganda a organisé ce 31 mars 2026 un atelier consacré à l'élaboration d'une norme de cybersécurité spécifique aux PME. L'élaboration de cette norme de cybersécurité spécifique aux PME offrira plusieurs avantages à l'environnement entrepreneurial de l'Ouganda. Pour les autorités de la NITA-U, cette initiative apparaît comme un levier structurant les PME digitales. Un tel référentiel permettrait de renforcer la confiance des

partenaires et des clients tout en garantissant la continuité des activités face aux incidents. Il va contribuer également à réduire les coûts liés aux cyberattaques et à simplifier les exigences de conformité souvent perçues comme complexes et contraignantes pour les petites structures.
https://cybersecuritymag.africa/cybersecurite-des-pme-en-ouganda-vers-une-norme-adaptee/

4. **Le Togo encadre la vidéosurveillance avec une plateforme numérique**
   L'Instance de Protection des Données à Caractère Personnel (IPDCP) du Togo a officiellement lancé le 27 mars 2026 une plateforme numérique dédiée à la déclaration en ligne des dispositifs de vidéosurveillance et de vidéoprotection. La cérémonie de lancement s'est tenue à l'hôtel SARAKAWA à Lomé, en présence de responsables de l'administration publique et de représentants des secteurs concernés. Selon le Président de l'IPDCP Togo, le Colonel Bédiani BELEI, cette nouvelle plateforme vise à simplifier les formalités liées à la déclaration des caméras de surveillance afin de réduir les délais de traitement.
   https://cybersecuritymag.africa/le-togo-encadre-la-videosurveillance-avec-une-plateforme-numerique/

5. **Arnaques sentimentales en ligne : un présumé cyberescroc arrêté pour une fraude internationale de plus de 100 millions de dollars**
   Les Services de Police du Ghana et le Federal Bureau of Investigation (FBI) ont arrêté récemment Derrick Van Yeboah alias « Van ». Il est accusé d'escroqueries sentimentales en ligne et de fraudes à la messagerie professionnelle. Il a été reconnu coupable pour son rôle au sein d'une organisation cybercriminelle internationale ayant dérobé plus de 100 millions de dollars à ses victimes par le biais d'escroqueries sentimentales en ligne et de fraudes à la messagerie professionnelle.
   https://cybersecuritymag.africa/un-presume-cyberescroc-arrete-pour-une-fraude-internationale-de-100-millions-dollars/

6. **Extensions IA : le cheval de Troie dans votre navigateur**
   Le navigateur web est devenu l'interface centrale du travail numérique. Messagerie, collaboration, applications SaaS : une grande partie de l'activité professionnelle passe désormais par cet environnement. L'intelligence artificielle y fait aujourd'hui une entrée rapide, notamment sous la forme d'extensions capables de résumer des pages, analyser des documents ou automatiser certaines tâches. Ces outils promettent des gains de productivité considérables. Mais leur adoption rapide soulève également des questions de sécurité. Car pour fonctionner, ces extensions demandent souvent des autorisations étendues : accès aux pages consultées, au contenu copié, voire aux documents ouverts dans le navigateur.
   https://www.undernews.fr/reseau-securite/extensions-ia-le-cheval-de-troie-dans-votre-navigateur.html

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**.