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 Janvier 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	Une vulnérabilité a été découverte dans Microsoft Edge. Elle permet 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 143.0.3650.139	12/01/2026	CVE-2026-0628	143.0.3650.139 Télécharger	Mettre à jour le navigateur	N/A
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 à distance et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Firefox versions antérieures à 146.0.1	19/12/2025	CVE-2025-14861	146.0.1 Télécharger	Mettre à jour le navigateur	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Chrome	Une vulnérabilité a été découverte dans Google Chrome. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Chrome versions antérieures à 143.0.7499.192 pour Linux • Chrome versions antérieures à 143.0.7499.192/.193 pour Windows et Mac	07/01/2026	CVE-2026-0628	143.0.7499.192/ .193 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. Elles permettent à un attaquant de provoquer une atteinte à l'intégrité des données et un problème de sécurité non spécifié par l'éditeur.	09/01/2026	CVE-2025-40204	16 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20260034-1	N/A
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 exécution de code arbitraire, un contournement de la politique de sécurité et un déni de service.	09/01/2026	CVE-2025-40300	10 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:0271	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
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 18.04 ESM • Ubuntu 20.04 ESM	09/01/2026	CVE-2025-40018	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7922-4	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 systèmes affectés sont les suivants : • Pixel versions antérieures au correctif du 12 janvier 2026	13/01/2026	CVE-2025-48647	10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2026/2026-01-01?hl=fr	N/A
Vulnérabilité dans Google Android	Une vulnérabilité a été découverte dans Google Android. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Android toutes versions avant le correctif du 5 janvier 2026	08/01/2026	CVE-2025-54957	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2026/2026-01-01?hl=fr	N/A

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!. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Joomla! CMS versions 3.9.x à 5.x antérieures à 5.4.2 • Joomla! CMS versions 6.x antérieures à 6.0.2	07/01/2026	CVE-2025-63083	6.0.2 Télécharger	Mettre à jour le CMS	5.9

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité WordPress	Une vulnérabilité de type injection de scripts intersites (XSS) a été identifiée dans le plugin *LiteSpeed Cache*. Elle résulte d'un défaut de filtrage et d'échappement des entrées utilisateur, permettant l'injection et l'exécution de code JavaScript malveillant dans le navigateur des victimes. Cette vulnérabilité peut entraîner le vol de sessions, l'exécution d'actions à l'insu des utilisateurs et la compromission de comptes administrateurs.	30/12/2025	CVE-2025-12450	6.9 Télécharger	Télécharger la dernière version Mettre à jour le plugin Vider le cache après mise à jour	7.0
	Une vulnérabilité critique a été découverte dans le plugin *King Addons for Elementor* pour WordPress. Elle permet à un utilisateur authentifié disposant de privilèges faibles d'élever ses droits jusqu'au niveau administrateur, en raison d'un contrôle insuffisant des autorisations. Cette faille peut conduire à une compromission complète du site (prise de contrôle, injection de code, modification de la configuration).	31/12/2025	CVE-2025-8489	6.9 Télécharger	Télécharger la dernière version Mettre à jour le plugin Supprimer le plugin s'il n'est pas nécessaire	9.0

II.4 INTELLIGENCE ARTIFICIELLE

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans n8n	Une vulnérabilité a été découverte dans n8n. Elle permet à un attaquant distant non authentifié d'accéder à des fichiers présents sur le serveur hôte via l'exécution de certains workflows basés sur des formulaires et des webhooks publics. Cette faille peut entraîner la divulgation d'informations sensibles et faciliter une compromission plus étendue du système selon la configuration du déploiement.	07/01/2026	CVE-2026-21858	1.121.0 Télécharger	Mettre à jour n8n vers la version 1.121.0 ou ultérieure Restreindre ou désactiver temporairement les webhooks publics	10.0

II.5 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans MISP	Une vulnérabilité a été découverte dans MISP. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants : • MISP versions antérieures à 2.5.32	13/01/2026		2.5.32 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.misp-project.org/security/	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Multiples vulnérabilités dans Curl	De multiples vulnérabilités ont été découvertes dans Curl. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Curl versions 7.17.x à 8.x antérieures à 8.18.0	07/01/2025	CVE-2025-15224	25.10 Télécharger	Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs https://curl.se/docs/CVE-2025-14524.html	N/A
Vulnérabilité dans MariaDB	De multiples vulnérabilités ont été découvertes dans MariaDB. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • MariaDB versions 10.6.x antérieures à 10.6.24 • MariaDB versions 11.4.x antérieures à 11.4.9 • MariaDB versions 11.7.x antérieures à 11.7.2 • MariaDB versions 11.8.x antérieures à 11.8.4	07/11/2025	CVE-2025-30722	12.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mariadb.com/docs/server/security/securing-mariadb/security	6.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits VMware Tanzu Gemfire	De multiples vulnérabilités ont été découvertes dans VMware Tanzu Gemfire. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une injection de requêtes illégitimes par rebond (CSRF) et un contournement de la politique de sécurité. • Tanzu GemFire versions antérieures à 10.1.6 • Tanzu GemFire versions antérieures à 10.2.1	13/01/2026	CVE-2025-67735	10.1.6 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36759	6.5
Vulnérabilité dans les produits Axis	De multiples vulnérabilités ont été découvertes dans les produits Axis. Elles permettent à un attaquant de provoquer une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • Axis Camera Station Pro versions antérieures à 6.8 • Axis Device Manager versions antérieures à 5.32 • Axis OS (anciennement LTS) versions 6.x antérieures à	12/01/2026	CVE-2025-30025	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.axis.com/dam/public/f2/28/d2/cve-2025-30025pdf-en-US-517962.pdf	4.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	6.50.5.19 • Axis OS (anciennement LTS) versions 8.x antérieures à 8.40.66 • Axis OS Active Track versions 12.x antérieures à 12.3.4 • Axis OS LTS 2020 versions 9.x antérieures à 9.80.90 • Axis OS LTS 2022 versions 10.x antérieures à 10.12.270 • Axis OS LTS 2024 versions 11.x antérieures à 11.11.127					

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 libpcap 1.10.5-1 versions antérieures à 1.10.6-1 • azl3 nmap 7.95-2 • cbl2 libpcap 1.10.1-4 • cbl2 nmap 7.93-3	09/01/2026	CVE-2025-11964	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-11964	1.9
Vulnérabilités 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 injection SQL (SQLi).	08/01/2026	CVE-2025-5965	25.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://thewatch.centreon.com/latest-security-bulletins-64/cve-2025-5965-centreon-web-high-severity-5362	7.2

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Tenable Nessus Agent	Une vulnérabilité a été découverte dans Tenable Nessus Agent. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Nessus Agent versions 11.x antérieures à 11.0.3 • Nessus Agent versions antérieures à 10.9.3	08/01/2026	CVE-2025-36640	11.0.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2026-01	7.3
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 18.7.x antérieures à 18.7.1	08/01/2025	CVE-2025-9222	18.7.1 Parcourir	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2026/01/07/patch-release-gitlab-18-7-1-released/	8.7

II.1 ACTUALITES

1. **Secteur sanitaire au Maroc : le ministère de la santé lance un SOC**
   Le Ministère de la Santé et de la Protection sociale du Maroc a lancé au mois de décembre dernier, un appel d'offres pour la mise en place d'un Centre d'Opérations de Sécurité Informatique (SOC). Ce centre aura la charge de surveiller en continu les systèmes d'information, de détecter les incidents et d'y répondre rapidement. Le projet s'accompagne d'un investissement estimé à plus de 10 millions de dirhams soit environ 1,10 million USD. L'ouverture des plis est prévue pour le 22 janvier 2026, ce qui laisse envisager un déploiement opérationnel courant 2026. Au-delà de la dimension technique, ce futur centre devra aussi contribuer à une meilleure gouvernance numérique du Ministère. Il s'agira notamment d'anticiper les risques, de renforcer les capacités internes et d'améliorer la résilience globale des infrastructures face à des attaques de plus en plus sophistiquée.
   https://cybersecuritymag.africa/secteur-sanitaire-au-maroc-le-ministere-de-la-sante-lance-bientot-un-security-operations-center-soc/

2. **Kaspersky présente ses prévisions cyber pour 2026 lors d'un prochain webinaire**

   Les équipes de recherche de Kaspersky (GReAT Global Research & Analysis Team) publient chaque année leurs prévisions sur les menaces cyber à venir. Pour 2026, leurs analyses s'appuient sur l'étude de centaines d'attaques observées dans le monde, dont plusieurs ont directement touché des acteurs africains. Pour présenter ces résultats, Georgy Kucherin, Senior Security Researcher chez Kaspersky, animera un webinaire en français de 45 minutes le mardi 20 janvier à 14h30 (CET). Lors de cette session, il reviendra sur les prédictions 2025 pour identifier ce qui s'est confirmé ou non. Il présentera les cybermenaces attendues en 2026 et fournira des clés de lecture utiles pour comprendre les enjeux en Afrique. Il partagera également des éléments concrets et pédagogiques pour aider les analystes, journalistes et experts à enrichir leurs articles ou décryptages.
   https://cybersecuritymag.africa/kaspersky-presente-ses-previsions-cyber-pour-2026-lors-dun-prochain-webinaire/

3. **Escroqueries sentimentales à grande échelle : le FBI et les autorités ghanéennes interpellent l'influenceur Abu Trica**
   L'Office ghanéen de Lutte contre la Criminalité Économique et le Crime Organisé et le FBI ont procédé ce 11 décembre 2025 à l'interpellation de Frederick Kumi plus connu sous le pseudonyme d'« Abu Trica ». L'information a été rendue publique par l'Office dans un communiqué en date du 12 décembre 2025 sur sa page officielle Facebook. Cette arrestation s'inscrit dans

une série d'actions judiciaires qui visent des ressortissants ghanéens impliqués dans des escroqueries sentimentales à grande échelle. Il a escroqué plus de 8 millions de dollars US à ces victimes. Selon l'Office, l'influenceur, suivi par des dizaines de milliers d'abonnés sur Instagram, est accusé d'avoir participé à un système d'escroquerie sentimentale en ligne ayant ciblé principalement des personnes âgées aux États-Unis. L'opération a été menée conjointement par les autorités ghanéennes, Interpol et le Federal Bureau of Investigation (FBI) américain à Accra. Par ailleurs, l'enquête a duré plusieurs mois et a également permis de remonter un réseau actif depuis 2023 à en croire les éléments de l'Office. Plus loin, les enquêteurs décrivent une mécanique désormais bien rodée. De faux profils souvent alimentés par des outils d'intelligence artificielle établissent des relations affectives sur les réseaux sociaux. La confiance s'installe.
https://cybersecuritymag.africa/escroqueries-sentimentales-a-grande-echelle-le-fbi-et-les-autorites-ghaneennes-interpellent-influenceur-abu-trica/

4. **Opération Sentinel en Afrique : 574 cybercriminels arrêtés lors d'une opération coordonnée par INTERPOL**
INTERPOL a annoncé le 19 décembre 2025 l'arrestation de 574 suspects cybercriminels et récupéré environ 03 millions de dollars US dans le cadre d'une importante opération de cybercriminalité à travers l'Afrique. Baptisée Opération Sentinel (27 octobre à 27 novembre 2025), elle a réuni les forces de l'ordre de 19 pays. Selon INTERPOL, l'opération s'est concentrée sur trois types de vecteurs de cybercriminalité. Il s'agit de Compromission des e-mails professionnels (BEC), de l'extorsion numérique et des ransomwares. Il faut préciser qu'au cours de cette opération coordonnée par INTERPOL, plus de 6 000 liens malveillants ont été supprimés et six variantes distinctes de ransomwares ont été décryptées. Par ailleurs, les cas examinés au cours de l'opération d'un mois étaient liés à des pertes financières estimées à plus de 21 millions de dollars US, selon les enquêteurs.
https://cybersecuritymag.africa/operation-sentinel-en-afrique-574-cybercriminels-arretes-lors-une-operation-coordonnee-par-interpol/
5. **Le propriétaire d'un Wifi peut-il vous espionner ?**
Après avoir lu cet article, vous réfléchirez peut-être à deux fois avant d'utiliser Wifi, en particulier s'il s'agit d'un Wifi public. Vous l'ignorez peut-être, mais il est tout à fait possible pour le propriétaire d'un Wifi (public ou non) de suivre les connexions sur son réseau, à condition d'avoir le bon équipement et le bon logiciel. D'ailleurs cela ne requiert parfois pas de connaissances techniques avancées, puisque la possibilité d'obtenir un historique des connexions des appareils clients est intégrée directement à une fonctionnalité (facile à utiliser) sur certains routeurs.
https://www.presse-citron.net/le-proprietaire-dun-wifi-peut-il-vous-espionner-reponse/

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**.