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 2025

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 autres 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 une exécution de code arbitraire à distance, 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 133.0.3065.51 ➢ Microsoft Edge pour iOS versions antérieures à 133.0.3065.51 ➢ Microsoft Edge versions antérieures à 133.0.3065.51	07/02/2025	CVE-2025-21408	133.0.3065.51 Télécharger	Mettre à jour le navigateur	8.8

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 133.0.6943.53 sur Linux ➢ Chrome versions antérieures à 133.0.6943.53/54 sur Windows et Mac	05/02/2025	CVE-2025-0451	132.0.6834.110/ 111 Télécharger	Mettre à jour le navigateur	6.3

II.2 SYSTÈMES D'EXPLOITATION

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 un problème de sécurité non spécifié par l'éditeur.	07/02/2025	CVE-2024-50275	9.4 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:1068	7.0
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 une exécution de code arbitraire, un déni de service et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Ubuntu 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 20.04 LTS • Ubuntu 24.10	07/02/2025	CVE-2024-53164	Ubuntu 24.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7238-3	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Pixel	Une vulnérabilité a été découverte dans Google Pixel. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Pixel toutes versions sans le correctif du 5 février 2025	05/02/2025	CVE-2025-0085	9 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2025-02-01?hl=fr	RESERVED
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Google indique que la vulnérabilité CVE-2024-53104 est activement exploitée dans le cadre d'attaques ciblées. Les systèmes affectés sont les suivants : • Android versions 12, 12L, 13, 14 et 15 sans le correctif de sécurité du 3 février 2025	04/02/2025	CVE-2025-20636	15 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2025-02-01?hl=fr	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités 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. Microsoft indique que les vulnérabilités CVE-2025-21391 et CVE-2025-21418 sont activement exploitées.	12/02/2025	CVE-2025-21420	Microsoft Windows 11	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21420	7.8

II.4 AUTRES

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. 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 versions affectées sont les suivantes : • Firefox ESR versions antérieures à 115.20 • Firefox ESR versions antérieures à 128.7 • Firefox versions antérieures à 135 • Thunderbird ESR versions antérieures à 128.7 • Thunderbird versions antérieures à 115.20 • Thunderbird versions antérieures à 135	05/02/2024	CVE-2025-1020	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2025-11/	9.8

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 atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.6.x antérieures à 17.6.5 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.7.x antérieures à 17.7.4 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.8.x antérieures à 17.8.2	12/02/2025	CVE-2025-1212	17.8.2 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2025/02/12/patch-release-gitlab-17-8-2-released/	4.3

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 une exécution de code arbitraire à distance, une élévation de privilèges et un contournement de la politique de sécurité.	12/02/2025	CVE-2025-24042		Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-24042	7.3
Vulnérabilités dans Microsoft Azure	Une vulnérabilité a été découverte dans Microsoft Azure. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions affectées sont les suivantes : • Azure Network Watcher VM Extension versions antérieures à 1.4.3563.1	12/02/2025	CVE-2025-21188	1.4.3563.1	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21188	6.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Adobe	De multiples vulnérabilités ont été découvertes dans les produits Adobe. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. L'éditeur indique que la vulnérabilité CVE-2025-24434 fait l'objet d'un correctif spécifique pour Commerce et Magento.	12/02/2025	CVE-2025-24438	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://helpx.adobe.com/security/products/magento/apsb25-08.html	8.7
Vulnérabilités dans Nginx	Une vulnérabilité a été découverte dans Nginx. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Nginx versions 1.11.4 à 1.x antérieures à 1.26.3 • Nginx versions 1.27.x antérieures à 1.27.4	11/02/2025	CVE-2025-23419	1.27.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mailman.nginx.org/pipermail/nginx-announce/2025/NYEUJX7NCBCGJGXDFVXNMAAMJDFSE45G.html	5.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Kaspersky	Une vulnérabilité a été découverte dans Kaspersky. Elle permet à un attaquant de provoquer une atteinte à l'intégrité des données.	07/02/2025	CVE-2024-13614	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.kaspersky.com/vulnerability/list-of-advisories/12430#060225	5.3
Vulnérabilités dans les produits Synology	Une vulnérabilité a été découverte dans les produits Synology. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • DSM 7.1.x toutes versions • DSM versions 7.2.x antérieures à 7.2.2-72806-3	05/02/2025	CVE-2024-56497	7.2.2-72806-3 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-23-189	6.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Multiples vulnérabilités dans les produits HPE Aruba Networking	De multiples vulnérabilités ont été découvertes dans les produits HPE Aruba Networking. 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 un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • HPE Aruba Networking ClearPass Policy Manager versions 6.11.x antérieures à 6.11.10 • HPE Aruba Networking ClearPass Policy Manager versions 6.12.x antérieures à 6.12.4	09/01/2025	CVE-2025-25039	134 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworks.com/2025/hpe_aruba_networking_-_hpesbnw04784.txt	4.7

II.3 ACTUALITES

1. **Forum Africain de la Cybersécurité : Le Maroc appelle à une coopération renforcée contre les cybermenaces**
   Le Forum Africain de la Cybersécurité a débuté ce lundi 03 février 2025 à Rabat au Maroc. L'événement qui se poursuit jusqu'au 05 février, réunit des experts et des responsables gouvernementaux pour aborder les enjeux de la cybersécurité en Afrique. Placé sous le thème « la transformation numérique de l'Afrique : adopter la cybersécurité et la souveraineté technologique », il a permis de discuter des défis géopolitiques et des cyberattaques sophistiquées. Un accent particulier a aussi été mis sur la nécessité d'une collaboration internationale renforcée.
   https://cybersecuritymag.africa/forum-africain-cybersecurite-au-maroc

2. **Attention aux offres d'emploi frauduleuses : le CERT Togo sonne l'alerte**
   Après le Bénin, une escroquerie en ligne frappe le Togo. Le Centre National de Réponse aux Incidents de Cybersécurité du Togo (CERT.tg) a émis une alerte sur des fraudes orchestrées via les réseaux sociaux et les applications de messagerie, notamment WhatsApp, Telegram, Facebook et TikTok. D'après le CERT.tg, les cybercriminels se font passer pour une société fictive baptisée « G » ou « Agence G » et proposent des opportunités d'emploi alléchantes. Le principe est simple : rédiger de faux avis sur Google Maps en échange d'une rémunération. Une fois les victimes attirées, les fraudeurs demandent des informations personnelles et, dans certains cas, incitent à verser une somme d'argent sous prétexte de frais d'activation. Les autorités togolaises ont identifié plusieurs numéros associés à cette escroquerie, principalement enregistrés au Nigeria, en Afrique du Sud et au Bangladesh. Les individus derrière cette fraude opèrent sous divers pseudonymes et usent de tactiques persuasives pour piéger leurs cibles.
   https://cybersecuritymag.africa/attention-aux-offres-emploi-frauduleuses-au-togo

3. **L'Algérie lance une campagne nationale pour sensibiliser les enfants des dangers du numérique**

   Le Ministre de la Poste et des Télécommunications de l'Algérie, Sid Ali Zerrouki, a présidé ce samedi 08 février 2025 à Alger le lancement officiel de la campagne nationale de sensibilisation sur la protection des enfants contre les dangers d'internet. Organisée en partenariat avec le Ministère de la Défense nationale, l'Agence de Sécurité des Systèmes d'Information, la Gendarmerie nationale et la Sûreté nationale, cette initiative vise à lutter contre les menaces numériques pesant sur les plus jeunes.

   https://cybersecuritymag.africa/algerie-lance-campagne-nationale-pour-sensibiliser-les-enfants-des-dangers-du-numerique

4. **Gestion des incidents cyber : ANSSI-Côte d'Ivoire lance ses activités en ligne**
   La Côte d'Ivoire a officialisé ce mardi 11 février 2025, le lancement en ligne des activités de l'Agence Nationale de la Sécurité des Systèmes d'Information de Côte d'Ivoire (ANSSI-Côte d'Ivoire). Ce lancement intervient dans le cadre de la Journée internationale pour un Internet plus sûr. Née le 30 octobre 2024 dernier de la vision conjointe du Ministère ivoirien de la Transition Numérique et de la Digitalisation et celui de l'Intérieur, l'ANSSI-Côte d'Ivoire incarne désormais le fer de lance de la cybersécurité ivoirienne. Elle centralise les missions de la DITT (incluant PLCC, CFAD, ALERTES100) et de l'ARTCI (audits, CI-CERT, PKI). L'ANSSI-Côte d'Ivoire se dote d'un arsenal complet pour contrer les cybermenaces.
   https://cybersecuritymag.africa/gestion-des-incidents-cyber-anssi-cote-ivoire-lance-ses-activites-en-ligne

5. **Rapport Google Cloud Security : « Comment les États-nations coopèrent de plus en plus avec des groupes cybercriminels »**
   Le rapport explique comment la cybercriminalité est devenue une force déstabilisatrice qui menace la sécurité nationale. En 2024, Mandiant (une entité de Google Cloud Security) a répondu à près de quatre fois plus d'intrusions menées par des acteurs à motivation financière que par des groupes soutenus par l'État. Le rapport met en lumière les points suivants :
   Comment "les quatre grands" utilisent la cybercriminalité comme une ressource et à des fins lucratives.La Russie, la Chine et l'Iran se sont tous appuyés sur la cybercriminalité pour mener à bien leurs opérations d'espionnage soutenues par l'État. En outre, les groupes d'espionnage iraniens et chinois ont déployé des ransomwares pour compléter leurs revenus. Enfin, la Corée du Nord mène désormais principalement des opérations à motivation financière, afin de collecter de l'argent pour soutenir le régime :
   https://www.undernews.fr/reseau-securite/rapport-google-cloud-security-comment-les-etats-nations-cooperent-de-plus-en-plus-avec-des-groupes-cybercriminels.html

6. **Vidspam, la nouvelle arnaque des cybercriminels**
   Les chercheurs de Proofpoint ont récemment publié une analyse sur l'évolution des arnaques liées aux cryptomonnaies, qui utilisent désormais des vidéos, en plus des photos, dans les messages MMS pour tromper leurs victimes.
   Tribune Proofpoint – Ce type d'attaque, appelé Vidspam, consiste à envoyer des fichiers vidéo de petite taille (.3gp), d'environ 14 Ko, pour tromper les victimes en les incitant à cliquer sur des liens renvoyant vers des groupes WhatsApp. Ces vidéos de faible qualité, qui ne contiennent aucune animation mais apparaissent comme des images fixes, servent à ajouter de la crédibilité aux messages et à inciter les utilisateurs à interagir.
   https://www.undernews.fr/reseau-securite/phishing-hoax/vidspam-la-nouvelle-arnaque-des-cybercriminels.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**.