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 Mai 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. 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 versions affectées sont les suivantes : • Microsoft Edge pour Android versions antérieures à 148.0.3967.55 • Microsoft Edge versions antérieures à 148.0.3967.55	12/05/2026	CVE-2026-8020	147.0.3912.87 Télécharger	Mettre à jour le navigateur	5.3
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 148.0.7778.167 pour Linux • Chrome versions antérieures à	13/05/2026		147.0.7727.137 Télécharger	Mettre à jour le navigateur	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	148.0.7778.167 pour Window • Chrome versions antérieures à 148.0.7778.168 pour Mac					
Vulnérabilité critique dans Apple Safari	De multiples vulnérabilités ont été découvertes dans Apple Safari. 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 versions affectées sont les suivantes : • Safari versions antérieures à 26.5	15/05/2026	CVE-2026-43660	26.5 Télécharger	Mettre à jour le navigateur	7.5
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Firefox versions antérieures à 150.0.3	13/05/2026	CVE-2026-8401	150.0.3 Télécharger	Mettre à jour le navigateur	9.5

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 un déni de service et un problème de sécurité non spécifié par l'éditeur.	15/05/2026	CVE-2026-43500	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20261858-1	7.8
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.	15/05/2026	CVE-2026-43284	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:16328	8.8

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. 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 18.04 ESM • Ubuntu 20.04 ESM • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS • Ubuntu 25.10	24/04/2026	CVE-2026-23411	26.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8180-5	7.8
Vulnérabilité dans Google Android	Une vulnérabilité a été découverte dans Google Android. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : • Android versions antérieures à 14, 15, 16 et 16-qpr2 avant le correctif du 4 mai 2026	05/05/2026	CVE-2026-0073	16 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2026/2026-05-01?hl=fr	8.8

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. Elles permettent à un attaquant de provoquer une élévation de privilèges, un déni de service à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Debian bookworm versions antérieures à 6.1.170-3 • Debian bullsey versions antérieures 5.10.251-4 • Debian bullsey versions antérieures à 6.1.170-3~deb11u1 • Debian trixie versions antérieures à 6.12.86-1	15/05/2026	CVE-2026-43500	13 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00169.html	7.8
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.	13/05/2026	CVE-2026-42899	11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42899	7.5

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans SPIP	De multiples vulnérabilités ont été découvertes dans SPIP. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : • SPIP versions antérieures à 4.4.14	12/05/2026		4.4.14 Télécharger	Mettre à jour le CMS	

II.4 AUTRES

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 une atteinte à la confidentialité des données et un problème de sécurité non spécifié par l'éditeur.	15/05/2026	CVE-2026-41615	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41615	9.6
Vulnérabilité dans Microsoft Azure	Une vulnérabilité a été découverte dans Microsoft Azure. Elle permet à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • azl3 azurelinux-image-tools 1.2.0-2 versions antérieures à 1.3.0-2	15/05/2026	CVE-2026-33814	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33814	7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Exchange Server	Une vulnérabilité a été découverte dans Microsoft Exchange Server. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Microsoft indique que la vulnérabilité CVE-2026-42897 est activement exploitée. Les systèmes affectés sont les suivants : • Microsoft Exchange Server 2016 Cumulative Update 23 • Microsoft Exchange Server 2019 Cumulative Update 14 • Microsoft Exchange Server 2019 Cumulative Update 15 • Microsoft Exchange Server Subscription Edition RTM	15/05/2026	CVE-2026-42897	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42897	8.1
Vulnérabilité dans PostgreSQL	De multiples vulnérabilités ont été découvertes dans PostgreSQL. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, un déni de service à distance et une atteinte à la confidentialité des	15/05/2026	CVE-2026-23561	18.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.postgresql.org/about/news/postgresql-184-1710-1614-1518-	3.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	données. Les systèmes affectés sont les suivants : • PostgreSQL versions 14.x antérieures à 14.23 • PostgreSQL versions 15.x antérieures à 15.18 • PostgreSQL versions 16.x antérieures à 16.14 • PostgreSQL versions 17.x antérieures à 17.10 • PostgreSQL versions 18.x antérieures à 18.4				and-1423-released-3297/	
Vulnérabilité dans les produits Cisco	De multiples vulnérabilités ont été découvertes dans les produits Cisco. 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. Cisco indique que la vulnérabilité CVE-2026-20182 est activement exploitée. Les systèmes affectés sont les suivants : • Catalyst SD-WAN versions 26.1.x antérieures à 26.1.1.1	15/05/2026	CVE-2026-20224	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW	8.6

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Intel	De multiples vulnérabilités ont été découvertes dans les produits Intel. 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.	13/05/2026		Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01457.html	
Vulnérabilité 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 exécution de code arbitraire à distance, un déni de service à distance et une atteinte à l'intégrité des données.	13/05/2026	CVE-2026-34686	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://helpx.adobe.com/security/products/magento/apsb26-49.html	8.7
Vulnérabilité dans Xen	Une vulnérabilité a été découverte dans Xen. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Xen versions 4.21.x sans le correctif de sécurité xsa490-4.21.patch • Xen versions xen-unstable sans le correctif de sécurité xsa490.patch	13/05/2026	CVE-2025-54518	8.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://xenbits.xen.org/xsa/advisory-490.html	7.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. 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.	13/05/2026	CVE-2026-44279	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-26-138	5.5
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, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Tomcat versions 11.0.x antérieures à 11.0.22	13/05/2026	CVE-2026-43515	11.0.22 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.55	9.1

II.1 ACTUALITES

1. **Le Liberia renforce son dispositif de cybersécurité avec un laboratoire d'investigation numérique**
   Le Liberia a mis en place une nouvelle infrastructure dédiée à la cybersécurité et aux enquêtes numériques. Cette initiative a pour objectif de renforcer la capacité du pays à faire face à la progression des menaces dans l'espace digital. Le dispositif repose sur un laboratoire spécialisé équipé d'outils d'analyse forensique et de détection des attaques informatiques. Il doit également appuyer les autorités dans le traitement des incidents cyber et la constitution de preuves numériques exploitables dans les enquêtes. Une délégation de la CEDEAO a effectué une visite d'inspection de l'infrastructure le mardi 12 mai 2026.
   https://cybersecuritymag.africa/le-liberia-renforce-son-dispositif-de-cybersecurite-avec-un-laboratoire-dinvestigation-numerique/

2. **Sécurité nucléaire : le Maroc maintient sa mobilisation face aux menaces cyber à Vienne**
   Lors d'une rencontre à l'occasion du 10ème anniversaire de la Déclaration commune sur l'atténuation des menaces internes à Vienne (Autriche), le Maroc a réaffirmé sa volonté de renforcer la sécurité nucléaire internationale face à la montée des menaces liées à la cybersécurité et à l'intelligence artificielle. Organisée avec l'Agence Internationale de l'Energie Atomique ; l'Agence Fédérale Belge de Contrôle Nucléaire et l'Administration Nationale de la Sécurité Nucléaire des États-Unis, cette rencontre visait à partager des expériences et à réfléchir aux réponses communes face aux nouvelles menaces numériques.
   https://cybersecuritymag.africa/le-maroc-maintient-mobilisation-menaces-cyber-nucleaire-a-vienne/

3. **Opération Ramz : Interpol démantèle des infrastructures criminelles numériques dans 13 pays**
   Une action coordonnée contre les réseaux de cybercriminalité au Moyen-Orient et en Afrique du Nord a conduit à l'identification de milliers de victimes et à l'interpellation de centaines de suspects. L'opération, baptisée « Ramz », a mobilisé les services de police de 13 pays entre octobre 2025 et février 2026, sous la coordination d'Interpol. Selon l'organisation internationale de police criminelle, l'opération visait à neutraliser des infrastructures numériques utilisées à des fins frauduleuses et à retrouver des individus impliqués dans des escroqueries en ligne ayant provoqué d'importantes pertes financières dans la région.
   https://cybersecuritymag.africa/operation-ramz-interpol-demantele-des-infrastructures-criminelles-numeriques-dans-13-pays/

4. **Le Maroc et le Ghana renforcent leur collaboration sur la gouvernance des données**
   Le Maroc et le Ghana ont signé le 7 mai 2026 à Rabat, une déclaration d'intention visant à renforcer leur coopération dans les domaines de l'administration digitale et de la réforme des services publics. L'accord a été conclu en marge des Assises Africaines du Gouvernement ouvert. Il prévoit un partage d'expertises entre les deux États autour de plusieurs axes notamment dans les domaines de la digitalisation, du gouvernement ouvert, de l'intelligence artificielle, de la gouvernance des données et des technologies émergentes, tout en soutenant l'inclusion numérique. Rabat et Accra veulent également développer des initiatives conjointes à travers des ateliers, des programmes de formation, des missions d'experts ainsi que des rencontres techniques destinées à favoriser l'innovation dans les administrations publiques
   https://cybersecuritymag.africa/le-maroc-et-le-ghana-renforcent-leurs-collaboration-sur-la-gouvernance-des-donnees/

5. **Cybersécurité aérienne : le Gabon sécurise davantage ses infrastructures critiques**
   Les autorités gabonaises ont récemment engagé une nouvelle collaboration visant à mieux protéger les systèmes d'information du secteur de l'aviation civile contre les cybermenaces. A ce sujet, l'Agence Nationale de l'Aviation Civile (ANAC) et l'Agence Nationale des Infrastructures Numériques et des Fréquences (ANINF) ont conclu un partenariat destiné à améliorer la cybersécurité des plateformes et équipements numériques liés au transport aérien. L'initiative prévoit notamment le renforcement de la protection des données sensibles, la modernisation des systèmes d'information ainsi qu'une meilleure résilience des infrastructures critiques face aux risques de cyberattaques ou de perturbations numériques. À travers cette coopération, le Gabon cherche également à favoriser une gestion plus sécurisée des échanges de données entre les différentes administrations impliquées dans l'aviation civile.
   https://cybersecuritymag.africa/cybersecurite-aerienne-le-gabon-securise-davantage-ses-infrastructures-critiques/

6. **Comment les hackers volent vos identifiants Active Directory**
   AD gère tout. Les comptes, les mots de passe, les accès, les politiques. Si vous compromettez un Domain Admin, vous avez le contrôle total de toutes les machines du domaine serveurs, postes de travail, tout. Le problème ? La plupart des environnements AD ont été configurés il y a dix ans et n'ont jamais été vraiment audités. Des comptes de service avec des mots de passe qui datent de 2015. Des utilisateurs avec des configurations Kerberos hasardeuses. Des droits accordés « temporairement » qui sont restés là pour toujours.
   https://www.undernews.fr/hacking-hacktivisme/comment-les-hackers-volent-vos-identifiants-active-directory.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**.