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 d'Avril 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 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	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 147.0.3912.87	29/04/2026	CVE-2026-6920	147.0.3912.87 Télécharger	Mettre à jour le navigateur	9.6
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 147.0.7727.137 pour Linux • Chrome versions antérieures à 147.0.7727.137 pour Windows • Chrome versions antérieures à 147.0.7727.138 pour Mac	29/04/2026	CVE-2026-7363	147.0.7727.137 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 SUSE	De multiples vulnérabilités ont été découvertes dans le noyau Linux de SUSE. 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.	24/04/2026	CVE-2026-5201	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20261583-1	7.5
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 un déni de service à distance.	24/04/2026	CVE-2026-23231	10.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:9870	7.8

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

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une injection SQL (SQLi) et une injection de requêtes illégitimes par rebond (CSRF). Les versions affectées sont les suivantes : • Moodle versions 4.5.x antérieures à 4.5.11 • Moodle versions 5.0.x antérieures à 5.0.7 • Moodle versions 5.1.x antérieures à 5.1.4	29/04/2026	CVE-2026-7278	5.2 Télécharger	Mettre à jour le CMS	R
Vulnérabilité dans Typo3	Une vulnérabilité a été découverte dans Typo3. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • typo3/cms-backend versions antérieures à 14.3.0 pour composer	21/04/2026	CVE-2026-6553	14.3.0 Télécharger	Mettre à jour le CMS	7.3

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité 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 postérieures ou égales à 7.10.6 et antérieures à 8.20.0	29/04/2026	CVE-2026-7168	8.20.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://curl.se/docs/CVE-2026-7168.html	R
Vulnérabilité dans les produits Foxit	De multiples vulnérabilités ont été découvertes dans les produits FoxIT. 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 systèmes affectés sont les suivants : • PDF Editor versions antérieures à 13.2.4 • PDF Reader versions 2026.x	27/04/2026	CVE-2026-5943	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.foxitsoftware.com/support/security-bulletins.php	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	antérieures à 2026.1.1 • PDF Reader versions antérieures à 14.0.4					
Vulnérabilité 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 systèmes affectés sont les suivants : • azl3 erlang 26.2.5.18-1 versions antérieures à 26.2.5.20-1 • azl3 lcms2 2.15-1 versions antérieures à 2.15-2 • azl3 vim 9.2.0240-1 versions antérieures à 9.2.0392-1	29/04/2026	CVE-2026-41411	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41411	6.6
Vulnérabilité dans Citrix XenServer	De multiples vulnérabilités ont été découvertes dans Citrix XenServer. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, un déni de service à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • XenServer versions 8.4 sans le dernier correctif de sécurité	29/04/2026	CVE-2026-23561	8.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696527&articleURL=XenServer_Security_Update_for_Multiple_Issues	R

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 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 : • Firefox ESR versions antérieures à 115.35.1 • Firefox ESR versions antérieures à 140.10.1 • Firefox versions antérieures à 150.0.1	29/04/2026	CVE-2026-7324	150.0.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2026-37/	7.3
Vulnérabilité dans Synolgy DSM	De multiples vulnérabilités ont été découvertes dans Synology DSM. 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 : • DSM versions 7.2.1-x antérieures à 7.2.1-69057-10 • DSM versions 7.2.2-x antérieures à 7.2.2-72806-7	24/04/2026	CVE-2026-32289	7.3.2-86009-2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.synology.com/en-global/security/advisory/Synology_SA_26_07	R

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• DSM versions 7.3.2-x antérieures à 7.3.2-86009-2					
Vulnérabilité dans Python	Une vulnérabilité a été découverte dans Python. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Python sans le dernier correctif de sécurité	28/04/2026	CVE-2026-5173	3.14.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/X6FXE5C6KDKOVNX3EC3DWD5RUPFWOZA4/	6.0
Vulnérabilité dans Zabbix Agent2	De multiples vulnérabilités ont été découvertes dans Zabbix Agent2. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Zabbix agent2 versions 7.4.8 et 7.4.9 sans les derniers correctifs de sécurité	27/04/2026	CVE-2026-32289	7.4.9 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.zabbix.com/browse/ZBX-27738	6.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft .Net	Une vulnérabilité a été découverte dans Microsoft .Net. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • ASP.NET Core 10.0 versions antérieures à 10.0.7	22/04/2026	CVE-2026-40372	10.0.7 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40372	9.1
Vulnérabilité dans Oracle Virtualization	De multiples vulnérabilités ont été découvertes dans Oracle Virtualization. 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 systèmes affectés sont les suivants : • Oracle VM VirtualBox version 7.2.6	22/04/2026	CVE-2026-35230	7.2.8 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.oracle.com/security-alerts/cpuapr2026.html	7.5

II.1 ACTUALITES

1. **Assainissement du cyberespace malien : le Procureur sort un communiqué officiel pour freiner des infractions observées**

   Dans un communiqué officiel en date du mardi 28 avril 2026, le Procureur du Pôle national de Lutte contre la Cybercriminalité a informé l'opinion publique des faits susceptibles de constituer des infractions à la loi pénale en matière de cybercriminalité au Mali. D'après le communiqué, plusieurs faits violant ladite loi ont été observés dans le cyberespace malien. Entre autres faits, il y a des appels à la haine et à la justice populaire, contraires au vivre ensemble et à la cohésion sociale ; des messages de désinformation, susceptibles de troubler l'ordre public, relayés sans fondement ; des informations tendancieuses de nature à interrompre le service public et le déroulement normal des cours au niveau des établissements d'enseignement et la circulation d'images et de vidéos sensibles et malveillantes.
   https://cybersecuritymag.africa/le-procureur-sort-un-communique-officiel-pour-freiner-des-infractions-observees/

2. **L'Éthiopie et le Mozambique concluent un partenariat sur les infrastructures numériques publiques**

   L 'Éthiopie et le Mozambique ont signé le 27 avril 2026 à Addis-Abeba, un protocole d'accord destiné à renforcer leur coopération dans le domaine de la transformation numérique. Paraphé entre FaydaVerse Digital Solutions Enterprise et l'Agence de transformation numérique et d'innovation du Mozambique, le texte prévoit la mise en place d'un cadre de collaboration technique axé sur le développement d'écosystèmes d'identité numérique sécurisés, inclusifs et interopérables.
   https://cybersecuritymag.africa/ethiopie-et-mozambique-concluent-un-partenariat-sur-les-infrastructures-numeriques-publiques/

3. **La GIZ recrute un conseiller régional en cybersécurité pour la CEDEAO**

   La Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) lance un appel à candidatures pour le poste de conseiller régional en cybersécurité en Afrique de l'Ouest, basé à Abuja. Ce recrutement vise à soutenir la CEDEAO dans le renforcement de ses capacités face aux cybermenaces. Le futur expert aura pour mission d'accompagner les politiques régionales de cybersécurité, de coordonner des projets et de favoriser la coopération entre les États membres.
   https://cybersecuritymag.africa/la-giz-recrute-un-conseiller-regional-en-cybersecurite-pour-la-cedeao/

4. **Renforcement des capacités en investigation numérique : Meta accompagne la montée en expertise de la Police sénégalaise**

Les enquêteurs des unités spécialisées de la Police du Sénégal ont bénéficié ce mardi 28 avril 2026 d'un programme de renforcement de capacités substantiel. Cette session de formation intensive vise à optimiser l'expertise des fonctionnaires de police en matière d'investigations numériques. Ce programme de formation a été animé par des experts du Groupe Meta. Selon la Police du Sénégal, ledit programme vient confirmer la collaboration entre elle et le Groupe Meta en matière de renforcement des capacités en matière des recherches et analyses numérique dans le pays.
https://cybersecuritymag.africa/meta-accompagne-la-montee-en-expertise-de-la-police-senegalaise/

5. **Fausse aide financière liée à la fête de l'indépendance au Togo : le CERT.tg appelle à la vigilance**

Le Centre national de réponse aux incidents de cybersécurité du Togo (CERT.tg) met en garde la population contre une nouvelle tentative d'arnaque qui circule actuellement sur les réseaux sociaux et les applications de messagerie. Il s'agit d'un message frauduleux qui affirme qu'une aide financière de 20 000 francs CFA serait offerte à tous les Togolais à l'occasion de la fête de l'indépendance. Le message invite les internautes à cliquer sur un lien et à répondre à un questionnaire pour recevoir immédiatement la somme annoncée. Dans certains cas, il est accompagné de faux témoignages de personnes prétendant avoir déjà bénéficié du transfert.
https://cybersecuritymag.africa/fausse-aide-financiere-liee-a-la-fete-de-lindependance-au-togo-le-cert-tg-appelle-a-la-vigilance/

6. **Une accélération de l'IA au détriment de la sécurité ? 41 % des entreprises françaises confrontées à des incidents liés à l'IA**

L'IA s'infiltre de plus en plus dans les organisations et est désormais opérationnelle dans la plupart des fonctions, avec des déploiements couvrant le support client, la messagerie interne, la messagerie électronique et la collaboration avec des tiers. 74 % des organisations françaises ont déployé des assistants IA au-delà de la phase pilote, et 72 % pilotent ou déploient activement des agents autonomes. Pourtant, alors que les organisations investissent dans les outils et les contrôles IA, beaucoup ne peuvent pas confirmer que ces contrôles sont efficaces : 78 % ne sont pas totalement convaincues que leurs contrôles de sécurité de l'IA permettraient de détecter une IA compromise, et 41% de celles qui ont mis en place des contrôles ont déjà connu un incident lié à l'IA confirmé ou suspecté.
https://www.undernews.fr/reseau-securite/une-acceleration-de-lia-au-detriment-de-la-securite-41-des-entreprises-francaises-confrontees-a-des-incidents-lies-a-lia.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. L'authentification multi facteur (MFA) reste l'un des mécanismes de protection les plus efficaces contre le vol de comptes. Des campagnes récentes ont démontré que des attaquants parviennent à dérober des jetons d'authentification en redirigeant les victimes vers des domaines malveillants via des services de messagerie légitimes. Nous invitons tous les organismes à activer la MFA sur l'ensemble de leurs comptes et services exposés, en particulier les accès administrateurs.
4. Une recrudescence des campagnes de phishing générées par intelligence artificielle est observée, capables d'imiter avec précision le style de communication des dirigeants. Ces attaques ciblent particulièrement les employés des services financiers, des ressources humaines et des directions générales. Nous recommandons de sensibiliser régulièrement vos collaborateurs et de n'entreprendre aucune action sensible (virement, partage d'accès, etc.) sur la seule base d'un courriel, sans vérification préalable par un autre canal.
5. Microsoft a mis fin au support de toutes les versions de Windows 10 depuis le 14 octobre 2025. Depuis cette date, les systèmes fonctionnant sous Windows 10 ne reçoivent plus le support technique, les mises à jour ni les correctifs de sécurité. Les systèmes non mis à jour sont particulièrement exposés aux logiciels malveillants, virus et autres formes de cyberattaques, car les vulnérabilités découvertes après cette date ne seront plus corrigées. Il est recommandé aux différents organismes de planifier la migration des postes utilisateurs fonctionnant encore sous Windows 10 vers Windows 11, en prenant en compte cette migration dans leurs prévisions budgétaires. Pour les postes ne répondant pas aux exigences techniques de Windows 11, il est conseillé de s'inscrire au programme Extended Security Updates (ESU) de Microsoft ou de procéder au remplacement du matériel concerné.

   https://support.microsoft.com/fr-fr/windows/windows-10-support-has-ended-on-october-14-2025-2ca8b313-1946-43d3-b55c-2b95b107f281
6. 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**.