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 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 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 133.0.3065.82	24/02/2025	CVE-2025-1006	133.0.3065.82 Télécharger	Mettre à jour le navigateur	8.8
Vulnérabilité dans Firefox	Une vulnérabilité a été découverte dans les produits Mozilla. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : • Firefox versions antérieures à 135.0.1	24/02/2025	CVE-2025-1414	135.0.1 Télécharger	Mettre à jour le navigateur	6.5

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 133.0.6943.141 pour Linux • Chrome versions antérieures à 133.0.6943.141/.142 pour Windows et Mac	26/02/2025		133.0.6943.141/ .142 Télécharger	Mettre à jour le navigateur	

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. 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 déni de service.	21/02/2025	CVE-2024-53113	9.4 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:1659	5.3
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 problème de sécurité non spécifié par l'éditeur.	28/02/2025	CVE-2024-53104	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20250713-1	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 exécution de code arbitraire, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Ubuntu 14.04 ESM • Ubuntu 16.04 ESM • Ubuntu 18.04 ESM • Ubuntu 20.04 LTS • Ubuntu 22.04 LTS • Ubuntu 24.04 LTS	28/02/2025	CVE-2025-0927	Ubuntu 24.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7308-1	N/A

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, une atteinte à la confidentialité des données et un déni de service. Les systèmes affectés sont les suivants : • Debian bookworm versions antérieures à 6.1.128-1	14/02/2025	CVE-2025-0927	6.1.128-1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2025/msg00023.html	5.5
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.3 Cms

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Drupal	De multiples vulnérabilités ont été découvertes dans Drupal. Certaines d'entre elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS), un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Drupal versions 10.4.x antérieures à 10.4.3 • Drupal versions 11.0.x antérieures à 11.0.12 • Drupal versions 11.1.x antérieures à 11.1.3 • Drupal versions antérieures à 10.3.13	20/02/2025		10.3.13 Explorer	Mettre à jour le navigateur	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla	Une vulnérabilité a été découverte dans Joomla!. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les versions affectées sont les suivantes : • Joomla! CMS versions 4.x antérieures à 4.4.11 • Joomla! CMS versions 5.x antérieures à 5.2.4	20/02/2025	CVE-2025-22207	5.2.4 Télécharger	Mettre à jour le navigateur	6.7

II.4 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Synologiy DSM	Une vulnérabilité a été découverte dans Synology DSM. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • DSM versions 7.1.x antérieures à 7.1.1-42962-8 • DSM versions 7.2.1.x antérieures à 7.2.1-69057-7 • DSM versions 7.2.2.x antérieures à 7.2.2-72806-3	28/02/2024		7.2.2-72806-3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.synology.com/fr-fr/security/advisory/Synology_SA_25_03	
Vulnérabilité dans Xen	Une vulnérabilité a été découverte dans Xen. Elle permet à un attaquant de provoquer un déni de service à distance. Les systèmes affectés sont les suivants : • Xen versions 4.x antérieures à 4.17.x sans le dernier correctif de sécurité	28/02/2025	CVE-2025-1713	17.8.2 télécharger	Veuillez-vous référer au Bulletin de sécurité : https://xenbits.xen.org/xsa/advisory-467.html	N/A

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans LibreOffice	Une vulnérabilité a été découverte dans LibreOffice. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • LibreOffice versions antérieures à 24.8.5	26/02/2025	CVE-2025-0514	25.2.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.libreoffice.org/about-us/security/advisories/cve-2025-0514/	7.2
Vulnérabilités dans GLPI	De multiples vulnérabilités ont été découvertes dans GLPI. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • GLPI versions antérieures à 10.0.18	26/02/2025	CVE-2025-21188	10.0.18 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://github.com/glpi-project/glpi/security/advisories/GHSA-vfxc-qg3v-j2r5	6.0

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans Wireshark	Une vulnérabilité a été découverte dans Wireshark. Elle permet à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes : • Wireshark versions 4.2.x antérieures à 4.2.11 • Wireshark versions 4.4.x antérieures à 4.4.4	20/02/2025	CVE-2025-1492	4.4.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.wireshark.org/security/wnpa-sec-2025-01.html	7.8
Multiples vulnérabilités dans OpenSSH	De multiples vulnérabilités ont été découvertes dans OpenSSH. 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 : • OpenSSH versions antérieures à 9.9p2	18/01/2025	CVE-2025-26466	9.9p2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.openssh.com/txt/release-9.9p2	5.9

II.4 ACTUALITES

1. **Madagascar amorce la création d'une Commission Malagasy de l'Informatique et des Libertés (CMIL)**
   L'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) et l'Organisation Internationale de la Francophonie (OIF) ont annoncé le 15 février 2025 d'accompagner Madagascar dans la création d'une Commission Malagasy de l'Informatique et des Libertés (CMIL). Ce projet s'inscrit dans la continuité des visites d'étude menées par des fonctionnaires malgaches au Maroc. Selon les délégations des deux organisations, cette mission va permettre à ce projet ambitieux de modernisation de l'administration malgache et de déployer l'e-gouvernance dans le pays. Le projet va offrir aux Malgaches un espace digital transparent et sécurisé, pilier essentiel d'une administration moderne et efficace.
   https://cybersecuritymag.africa/madagascar-amorce-la-creation-une-commission-malagasy-de-informatique-et-des-libertes-cmil

2. **Prévention et sécurité en ligne : l'APDP-Bénin sensibilise les élèves aux risques cyber**
   Dans le cadre d'une initiative ambitieuse, l'Autorité de Protection des Données Personnelles (APDP) Bénin a poursuivi ce vendredi 14 février, ses missions de sensibilisation au numérique. L'APDP-Bénin a rencontré les élèves du Complexe d'Enseignement Technique et Général BETHESDA à Cotonou. Cette rencontre s'inscrit dans une série de missions qui vise à promouvoir la citoyenneté numérique et à prévenir les risques liés aux mauvaises pratiques en ligne. Selon l'APDP-Bénin,

cette rencontre a été placée au cœur d'une série d'actions éducatives pour forger une génération consciente des enjeux du digital, de la protection des données personnelles et de la citoyenneté numérique dans le pays.
https://cybersecuritymag.africa/prevention-et-securite-en-ligne-lapdp-benin-sensibilise-les-eleves-aux-risques-cyber

3. **La PLCC et les instances de Police se mobilisent contre les menaces sexuelles et fake news à Abidjan**

   La Plateforme de Lutte Contre la Cybercriminalité (PLCC) en collaboration avec la Préfecture de Police d'Abidjan et la Police Nationale se mobilise davantage contre les menaces sexuelles en ligne et les fake news. C'est ce mercredi 26 février 2025, à l'occasion d'une journée portes ouvertes que la Préfecture de Police d'Abidjan, la Police Nationale et PLCC ont tenu une conférence sur « Les dangers des réseaux sociaux : cas des menaces sexuelles et fake news ». Selon les parties organisatrices de la conférence de sensibilisation, cette initiative s'inscrit dans le cadre de la lutte contre la cybercriminalité galopante dans le pays.

   https://cybersecuritymag.africa/plcc-et-instances-de-police-se-mobilisent-contre-les-menaces-sexuelles-et-fake-news

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. **Le Cameroun accueille son premier Hackathon de cybersécurité pour stimuler l'innovation et les talents locaux**
   Le Cameroun s'apprête à accueillir son premier Hackathon de cybersécurité local. Il s'agit d'une compétition destinée aux étudiants passionnés de technologie et experts du domaine. Prévu du 24 au 26 avril 2025 à Douala, cet événement se tiendra dans le cadre du Salon des métiers et innovations locales de cybersécurité sous le parrainage du Ministère de la Recherche Scientifique et de l'Innovation. Durant deux jours, les participants auront l'opportunité de relever des défis concrets en cybersécurité, afin de mettre à l'épreuve leurs compétences techniques et stratégiques. L'objectif est de renforcer les capacités locales en cybersécurité et de sensibiliser à la protection du cyberespace camerounais. En réalité, ce hackathon offrira aux étudiants et professionnels l'occasion de développer leurs compétences à travers la résolution de défis techniques en conditions

réelles. Il permettra également de rencontrer des experts du secteur et des recruteurs potentiels.
https://cybersecuritymag.africa/le-cameroun-accueille-son-premier-hackathon-de-cybersecurite

6. **L'IA au service de la protection des Datacenters**
Bien sûr, la majorité des Datacenters sont aujourd'hui équipés de systèmes leur permettant d'activer un certain nombre de protections en cas d'incendie. Pour autant, l'actualité nous montre que cette approche n'est pas suffisante et n'empêche pas les catastrophes de se produire, entrainant ensuite des conséquences désastreuses pour les entreprises qui ont hébergé leurs applications, systèmes d'information et données sur ces sites. C'est précisément pour cette raison qu'une approche 100 % réactive à incident n'est pas la bonne méthode et fait courir des risques inconsidérés aux exploitants de datacenters.

https://www.undernews.fr/reseau-securite/lia-au-service-de-la-protection-des-datacenters.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**.