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 Mars 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	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 134.0.3124.93	27/03/2025	CVE-2025-2783	134.0.3124.93 Télécharger	Mettre à jour le navigateur	NA
Vulnérabilité dans Mozilla Firefox	Une vulnérabilité a été découverte dans Mozilla Firefox. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Firefox ESR versions antérieures à 115.21.1 • Firefox ESR versions antérieures à 128.8.1 • Firefox versions antérieures à 136.0.4	28/03/2025	CVE-2025-2857	136.0.4 Télécharger	Mettre à jour le navigateur	NA

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 135.0.7049.41/42 pour Windows et Mac • Chrome versions antérieures à 135.0.7049.52 pour Linux	02/04/2025	CVE-2025-3074	135.0.7049.41/42 Télécharger	Mettre à jour le navigateur	NA

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 déni de service à distance, une atteinte à l'intégrité des données et un contournement de la politique de sécurité.	28/03/2025	CVE-2025-21785	10 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:3264	7.8
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 exécution de code arbitraire, une élévation de privilèges et une atteinte à la confidentialité des données.	28/03/2025	CVE-2025-21780	15 SP6 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20251027-1	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, un contournement de la politique de sécurité et un déni de service. 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 • Ubuntu 24.10	28/03/2025	CVE-2025-21834	Ubuntu 24.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7382-1	NA

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Drupal	Une vulnérabilité a été découverte dans Drupal. Elle permet à un attaquant de provoquer une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Drupal versions 11.0.x antérieures à 11.0.13 • Drupal versions 11.1.x antérieures à 11.1.5	20/03/2025		11.1.5 Télécharger	Mettre à jour le CMS	
Vulnérabilité dans Moodle	De multiples vulnérabilités ont été découvertes dans Moodle. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Moodle versions 4.5.x antérieures à 4.5.3	26/03/2025		4.5.3+ 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 Splunk	De multiples vulnérabilités ont été découvertes dans les produits Splunk. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • image docker splunk/splunk versions 9.4.x antérieures à 9.4.1 • image docker splunk/universalforwarder versions 9.4.x antérieures à 9.4.1	03/04/2024	CVE-2024-56326	9.4.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://advisory.splunk.com/advisories/SVD-2025-0402	5.4
Vulnérabilité dans Microsoft Azure	De multiples vulnérabilités ont été découvertes dans Microsoft Azure. Elles permettent à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • Azure Health Bot • Azure Playwright	01/04/2025	CVE-2025-26683	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-26683	8.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits VMware	Une vulnérabilité a été découverte dans les produits VMware. Elle permet à un attaquant de provoquer une élévation de privilèges. Les versions affectées sont les suivantes : • Aria Operations versions 8.x antérieures à 8.18 HF 5 • Cloud Foundation versions 4.x sans les derniers correctifs de sécurité • Cloud Foundation versions 5.x sans les derniers correctifs de sécurité • Telco Cloud Infrastructure versions antérieures à 8.18 HF 5 • Telco Cloud Platform versions antérieures à 8.18 HF 5	02/04/2025	CVE-2025-22331	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25541	7.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilités dans les produits Kaspersky	De multiples vulnérabilités ont été découvertes dans les produits Kaspersky. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Anti Targeted Attack Server versions 6.x antérieures à 6.0.4 • Anti Targeted Attack Server versions 7.x antérieures à 7.0.3 • IoT Secure Gateway Network Protector version 3.1.0.130 sans les derniers correctifs de sécurité	02/04/2025	CVE-2024-55629	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.kaspersky.com/vulnerability/list-of-advisories/12430#010425	7.5
Vulnérabilités dans les produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données.	01/04/2025	CVE-2021-24008	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-20-105	5.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Multiples vulnérabilités dans Zabbix	De multiples vulnérabilités ont été découvertes dans Zabbix. 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 SQL (SQLi). Les systèmes affectés sont les suivants : • Zabbix versions 5.0.x antérieures à 5.0.46rc1 • Zabbix versions 6.0.x antérieures à 6.0.39rc1 • Zabbix versions 7.0.x antérieures à 7.0.10rc1 • Zabbix versions 7.2.x antérieures à 7.2.4rc1	01/04/2025	CVE-2024-45700	7.2.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.zabbix.com/browse/ZBX-26258	6.0

II.4 ACTUALITES

1. **Sécurisation du cyberespace congolais : Oboulhas Tsahat Conrad Onésime prend la tête de l'ANSSI**
   Oboulhas Tsahat Conrad Onésime est le tout premier Directeur Général à la tête de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) du Congo. Il a été officiellement installé dans ses fonctions le 20 février 2025. La cérémonie a été présidée par Stevie Pea Ondongo, Ministre et Secrétaire Général de la Présidence de la République, en présence de Jean-Dominique Okemba, Secrétaire Général du Conseil National de Sécurité (CNS). Lors de son intervention, Jean Dominique Okemba a souligné que la création de l'ANSSI répond à la volonté du chef de l'État à renforcer la protection du cyberespace national. « La cybersécurité n'est plus une option, mais une nécessité absolue qui requiert la mobilisation de tous », a-t-il déclaré. Il a également précisé que le CNS assurera la supervision et la coordination des activités de l'Agence pour garantir son efficacité.
   https://cybersecuritymag.africa/index.php/oboulhas-tsahat-conrad-onesime-prend-la-tete-de-anssi-congo

2. **L'ASIN et le FIRST organisent un atelier de simulation de gestion de cybercrise à Cotonou**
   L'Agence des Systèmes d'Information et du Numérique du Bénin (ASIN-Bénin) et le Forum of Incident Response and Security Teams (FIRST) ont organisé vendredi 28 mars 2025, un atelier de simulation de gestion de cybercrise à Cotonou. Selon les organisateurs, cet atelier vise à forger une armure collective contre les pirates du numérique désormais plus agressifs que jamais. Au cours de l'atelier, M. Marc-André LOKO, Directeur Général de l'ASIN-Bénin a rappelé que les attaques informatiques ne sont plus une simple éventualité. Pour lui, elles sont une réalité quotidienne.
   https://cybersecuritymag.africa/lasin-et-le-first-organisent-un-atelier-de-simulation-de-gestion-de-cybercrise-cotonou

3. **La CIL-Burkina Faso lance la 3e édition de la Journée Nationale de Protection des Données à Caractère Personnel**

   La Commission de l'Informatique et des Libertés du Burkina Faso (CIL-Burkina Faso) a lancé le mardi 25 mars 2025, la 3e édition de la Journée Nationale de la Protection des Données à Caractère Personnel (JNPDP-2025). Du 25 au 28 mars 2025, cet événement est placé sous le thème : « La protection des données à caractère personnel à l'ère de la digitalisation des procédures administratives : quelle contribution des acteurs de l'écosystème du numérique ».

   https://cybersecuritymag.africa/index.php/la-cil-burkina-faso-lance-la-3-edition-de-la-journee-nationale-de-protection-des-donnees-caractere

4. **Les stratégies de réponse aux incidents de cybersécurité**
   Les cyberattaques se multiplient et évoluent avec une rapidité alarmante. Ceci expose les entreprises, institutions et particuliers à des risques croissants. Face à cette menace omniprésente, la mise en place de stratégies de réponse aux incidents de cybersécurité est devenue une priorité absolue. Une réaction rapide et efficace permet non seulement de limiter les impacts des attaques, mais aussi de renforcer la résilience des systèmes face aux menaces futures. Pour en parler, nous recevons Jean-Christophe Lutundula Apala, Ingénieur Sénior en cybersécurité. Il nous apporte son expertise sur les approches à adopter pour une gestion efficace des incidents et les défis que rencontrent les entreprises dans ce domaine.
   https://cybersecuritymag.africa/index.php/cyberinterview-jean-christophe-apala-les-strategies-de-reponse-aux-incidents-de-cybersecurite

5. **Microsoft lance Copilot Search : voici comment essayer ce nouveau moteur de recherche**
   Microsoft a-t-il, une fois de plus, devancé Google? Alors que la firme de Mountain View travaille toujours sur le mode IA de Google Search, Microsoft a discrètement lancé une nouvelle interface pensée pour l'ère de l'intelligence alternative. Cette nouvelle interface est baptisée Copilot Search et, comme le suggère le nom, elle permet d'utiliser Copilot pour faire des recherches en ligne. Contrairement au moteur de recherche classique Bing, Copilot Search se focalise sur le chatbot. Il permet de poser des questions à l'IA, qui répond directement, tout en partageant les sources utilisées pour créer ces réponses. En tout cas, cette version du moteur de recherche de Microsoft, entièrement propulsé par Copilot, n'inclut plus les résultats de recherche de Bing.
   https://www.presse-citron.net/microsoft-lance-copilot-search-voici-comment-essayer-ce-nouveau-moteur-de-recherche/

6. **Journée mondiale de la sécurité du cloud : l'importance cruciale de la protection des identités**
   Une sécurité efficace des identités dans le cloud garantit que seules les entités autorisées accèdent aux ressources spécifiques, réduisant ainsi les risques de violations de données et d'accès non autorisés. La gestion des identités sur différentes plateformes peut entraîner des politiques de sécurité incohérentes, augmentant ainsi les vulnérabilités. Par ailleurs, la prolifération des identités machines aux côtés des utilisateurs humains complique l'application des protocoles de sécurité. Enfin, maintenir un équilibre entre rapidité de développement et respect des mesures de sécurité strictes est un défi, souvent à l'origine de mauvaises configurations.
   https://www.undernews.fr/authentification-biometrie/journee-mondiale-de-la-securite-du-cloud-limportance-cruciale-de-la-protection-des-identites.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**.