**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 du mois de Janvier 2025

B.P. 6170 Tél : 694 405 868 Web : http//www.antic.cm ; Email : infos@antic.cm

# Sommaire


I. LEXIQUE DU BULLETIN ..... 4
II. VULNÉRABILITÉS PUBLIÉES ..... 5
II.1 NAVIGATEURS ..... 5
Vulnérabilité dans Microsoft Edge ..... 5
Vulnérabilité dans Mozilla Firefox pour iOS ..... 5
Vulnérabilité dans Google Chrome ..... 6
II.2 SYSTÈMES D'EXPLOITATION ..... 7
Vulnérabilité dans le noyau Linux de Red Hat ..... 7
Vulnérabilité dans le noyau Linux d'Ubuntu ..... 7
Vulnérabilité dans Google Pixel ..... 8
Vulnérabilité dans Google Android ..... 8
Vulnérabilités dans Microsoft Windows ..... 9
Vulnérabilité dans le noyau Linux de SUSE ..... 9
II.3 CMS ..... 10
Vulnérabilité dans SPIP ..... 10
Vulnérabilité dans Typo3 ..... 10
Vulnérabilité dans Joomla ! ..... 11
II.4 AUTRES ..... 12
Vulnérabilité dans les produits Mozilla ..... 12
Vulnérabilités dans les produits Microsoft ..... 13
Vulnérabilités dans Microsoft.Net. ..... 13

Vulnérabilités dans les produits Cisco ..... 13
Vulnérabilités dans ClamAV ..... 14
Vulnérabilités dans Oracle MySQL ..... 14
Vulnérabilités dans PHPMyAdmin ..... 15
Vulnérabilité dans les produits HPE Aruba Networking ..... 16
Vulnérabilités dans les produits Fortinet ..... 17
Multiples vulnérabilités dans Mozilla Thunderbird ..... 17
Vulnérabilité dans GitLab ..... 18
II.4 ACTUALITES ..... 19
III. NOTES IMPORTANTES ..... 21

# 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 contournement de la politique de sécurité. Les versions affectées sont les suivantes :<br>➢ Microsoft Edge versions antérieures à 132.0.2957.127 | 27/01/2025 | CVE-2025-21262 | 132.0.2957.127<br>Télécharger | Mettre à jour le navigateur | 5.4 |
| **Vulnérabilité dans Mozilla Firefox pour iOS** | De multiples vulnérabilités ont été découvertes dans Mozilla Firefox pour iOS. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes :<br>➢ Firefox pour iOS versions antérieures à 134 | 13/01/2025 | CVE-2025-23108 | 134<br>Télécharger | Mettre à jour le navigateur | 4.3 |

| 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 :<br>➢ Chrome Extended Stable versions antérieures à 132.0.6834.110/111 pour Windows et Mac<br>➢ Chrome versions antérieures à 132.0.6834.110 pour Linux<br>➢ Chrome versions antérieures à 132.0.6834.110/111 pour Windows et Mac | 23/01/2025 | CVE-2025-0612 | 132.0.6834.110/ 111<br>Télécharger | Mettre à jour le navigateur | N/A |

## 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 une atteinte à la confidentialité des données et un contournement de la politique de sécurité. | 24/01/2025 | CVE-2024-53088 | 9.4<br>Essayer | Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2025:0578 | 4.7 |
| **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 atteinte à la confidentialité des données, une atteinte à l'intégrité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants :<br>• Ubuntu 22.04 LTS<br>• Ubuntu 24.04 LTS | 24/01/2025 | CVE-2024-56757 | Ubuntu 24.04.01 LTS<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-7166-4 | 5.5 |

| 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 exécution de code arbitraire à distance. Les systèmes affectés sont les suivants :<br>• Google Pixel sans les correctifs de sécurité du 5 janvier 2025 | 08/01/2025 | CVE-2024-53842 | 9<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2025-01-01?hl=fr | 9.8 |
| **Vulnérabilité dans Google Android** | De multiples vulnérabilités ont été découvertes dans Google Android. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants :<br>• Android versions antérieures à 12, 12L, 13, 14 et 15 avant le correctif du 5 janvier 2025 | 03/01/2025 | CVE-2024-49749 | 15<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2025-01-01?hl=fr | 8.8 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilités dans Microsoft Windows** | Une vulnérabilité a été découverte dans Microsoft Windows. Elle permet à un attaquant de provoquer une élévation de privilèges. | 17/01/2025 | CVE-2025-21325 | Microsoft Windows 11 | Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21325 | 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. | 24/01/2025 | CVE-2024-8805 | 15 SP6 Télécharger | Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2025/suse-su-20250203-1 | 8.8 |

## II.3 CMS

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilité dans SPIP** | Une vulnérabilité a été découverte dans SPIP SPIP. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes :<br>➢ SPIP versions 4.1.x antérieures à 4.1.20<br>➢ SPIP versions 4.2.x antérieures à 4.2.17<br>➢ SPIP versions 4.3.x antérieures à 4.3.6 | 17/01/2025 | | 4.3.6<br>Télécharger | Mettre à jour le CMS | N/A |
| **Vulnérabilité dans Typo3** | De multiples vulnérabilités ont été découvertes dans les produits Typo3. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une injection de requêtes illégitimes par rebond (CSRF) et un contournement de la politique de sécurité. | 14/01/2025 | CVE-2025-23108 | 13.4.4<br>Télécharger | Mettre à jour le CMS | 4.3 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilité dans Joomla !** | De multiples vulnérabilités ont été découvertes dans Joomla!. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Les versions affectées sont les suivantes :<br>➢ Joomla! CMS versions 3.x-elts antérieures à 3.10.20-elts<br>➢ Joomla! CMS versions 4.x antérieures à 4.4.10<br>➢ Joomla! CMS versions 5.x antérieures à 5.2.3 | 08/01/2025 | CVE-2024-40749 | 5.2.3<br>Télécharger | Mettre à jour le CMS | 7.5 |

## 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 :<br>• Thunderbird versions antérieures à 128.4.3<br>• Thunderbird versions antérieures à 132.0.1 | 14/11/2024 | CVE-2024-11159 | Explorer | Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2024-62/ | 9.1 |

| 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. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. | 15/01/2025 | CVE-2025-21405 | | Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21405 | 7.3 |
| **Vulnérabilités dans Microsoft.Net.** | De multiples vulnérabilités ont été découvertes dans Microsoft .Net. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges. | 15/01/2025 | CVE-2025-21176 | | Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-21176 | 8.8 |
| **Vulnérabilités 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 et un déni de service à distance. | 23/01/2025 | CVE-2025-20165 | Explorer | Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-privesc-uy2Vf8pc | 7.5 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilités dans ClamAV** | Une vulnérabilité a été découverte dans ClamAV. Elle permet à un attaquant de provoquer un déni de service à distance. Les versions affectées sont les suivantes :<br>➢ ClamAV versions 1.0.x antérieures à 1.0.8<br>➢ ClamAV versions 1.4.x antérieures à 1.4.2 | 25/01/2025 | CVE-2025-20128 | Explorer | Veuillez-vous référer au Bulletin de sécurité : https://blog.clamav.net/2025/01/clamav-142-and-108-security-patch.html | 5.3 |
| **Vulnérabilités dans Oracle MySQL** | De multiples vulnérabilités ont été découvertes dans Oracle MySQL. 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. | 22/01/2025 | CVE-2025-21567 | 8.0.41 Télécharger | Veuillez-vous référer au Bulletin de sécurité : https://www.oracle.com/security-alerts/cpujan2025.html | 4.3 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilités dans PHPMyAdmin** | De multiples vulnérabilités ont été découvertes dans PHPMyAdmin. Elles permettent à un attaquant de provoquer une injection de code indirecte à distance (XSS) et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes :<br>➢ phpMyAdmin versions 5.x antérieurs à 5.2.2 | 22/01/2025 | CVE-2024-2961 | 5.2.2<br>Télécharger | Veuillez-vous référer au Bulletin de sécurité : https://www.phpmyadmin.net/security/PMASA-2025-3/ | 7.3 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilité dans les produits HPE Aruba Networking** | Une vulnérabilité a été découverte dans les produits HPE Aruba Networking. Elle permet 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 :<br>• AOS-CX versions 10.14.x antérieures à 10.14.1030<br>• AOS-CX versions 10.15.x antérieures à 10.15.1000<br>• AOS-CX versions antérieures à 10.13.1070<br><br>L'éditeur indique que les versions 10.10.x sont affectées mais ne bénéficieront pas de correctifs de sécurité. | 09/01/2025 | CVE-2024-54010 | 10.13.x Explorer | Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworks.com/2025/hpe_aruba_networking_-_hpesbnw04772.txt | 3.4 |

| Vulnérabilité | Description | Date de publication | Référence CVE | Dernière version | Solution | Score CVSS |
|---|---|---|---|---|---|---|
| **Vulnérabilités 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. | 15/01/2025 | CVE-2024-56497 | Explorer | Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-23-189 | 6.7 |
| **Multiples vulnérabilités dans Mozilla Thunderbird** | De multiples vulnérabilités ont été découvertes dans Mozilla Thunderbird. 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. Les systèmes affectés sont les suivants :<br>➢ Thunderbird ESR versions antérieures à 115.19<br>➢ Thunderbird ESR versions antérieures à 128.6<br>➢ Thunderbird versions antérieures à 134 | 09/01/2025 | CVE-2025-0247 | 134 Explorer | Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2025-05/ | 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 injection de code indirecte à distance (XSS). Les systèmes affectés sont les suivants :<br>➢ GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.6.x antérieures à 17.6.4<br>➢ GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.7.x antérieures à 17.7.3<br>➢ GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) versions 17.8.x antérieures à 17.8.1 | 23/01/2025 | CVE-2025-0314 | Explorer | Veuillez-vous référer au Bulletin de sécurité : https://about.gitlab.com/releases/2025/01/22/patch-release-gitlab-17-8-1-released/ | 8.7 |

## II.4 ACTUALITES

1. **Cyberrésilience au Tchad : ANSICE renforce ses capacités grâce aux nouveaux partenariats**
   L'Agence Nationale de la Sécurité Informatique et de Certification Électronique du Tchad (ANSICE-Tchad) renforce ses engagements en matière de cyber-résilience. C'est dans cette optique que l'ANSICE-Tchad s'est entretenu en réunion tripartite le lundi 13 janvier 2025 avec ses cadres dirigeants, la Banque Mondiale et le Cabinet Keystone en prélude à la deuxième mission de restitution de cyber-résilience prévue pour la fin du mois de janvier 2025 au Tchad. C'est sous la direction de Mlle Nadjma KEBZABO, Directrice Générale adjointe de l'ANSICE-Tchad que les discussions ont eues lieu.
   https://cybersecuritymag.africa/cyberresilience-au-tchad-ansice-renforce-ses-capacites-grace-aux-nouveaux-partenariats

2. **Nouvelle dynamique pour la cybersécurité en guinée : Création de l'Association des Professionnels de la Sécurité de l'Information de Guinée (APSI-GN)**
   Comme le Niger le 29 décembre 2024 dernier, un groupe d'experts en cybersécurité de la République de Guinée a annoncé le mercredi 15 janvier 2025, la création de l'Association des Professionnels de la Sécurité de l'Information de Guinée (APSI-Guinée). Une organisation à but non lucratif dédiée à la promotion et au renforcement des pratiques de cybersécurité en Guinée. À en croire le groupe, APSI-GN a pour mission d'une part de sensibiliser les entreprises, les organismes publics et la société civile à l'importance de la cybersécurité et de valoriser les métiers de la sécurité de l'information à travers un code de déontologie.
   https://cybersecuritymag.africa/creation-association-des-professionnels-de-securite-information-Guinee

3. **Fraude numérique au Burkina : La BCLCC interpelle un suspect pour appropriation illégale de fonds**

   La Brigade Centrale de Lutte Contre la Cybercriminalité (BCLCC) a interpellé D.I, un maçon de 28 ans domicilié à Ouagadougou, pour une appropriation illégale de 1 500 000 FCFA. En mai 2024, D.H, un orpailleur résidant au Mali, a transféré par erreur cette somme sur le compte de D.I, au lieu de celui de son collègue Z.H, basé au Burkina Faso. Cependant, malgré plusieurs sollicitations pour restituer l'argent, y compris une proposition de conserver 100 000 FCFA, D.I a refusé et a coupé tout contact. Z.H a alors déposé une plainte auprès de la BCLCC, qui a permis l'interpellation de D.I le 17 janvier 2025. Lors de son audition, D.I a admis avoir dépensé l'argent à des fins personnelles.

   https://cybersecuritymag.africa/bclcc-burkina-interpelle-un-suspect-pour-appropriation-illegale-de-fonds

4. **Young Women in Tech : Un programme de formation gratuite en cybersécurité pour les jeunes filles du Ghana**
   À l'occasion de la Journée internationale des femmes, la Fondation Slamm, en partenariat avec l'ISC2, lance un programme de formation gratuite en cybersécurité dédié aux jeunes femmes du Ghana. Baptisé Young Women in Tech, ce programme vise à réduire les écarts de représentation dans ce secteur tout en offrant aux participantes les outils nécessaires pour exceller dans le domaine. La formation se déroulera du 17 au 28 mars 2025, à Kumasi, au Ghana. Elle s'adresse essentiellement aux jeunes femmes âgées de 20 à 36 ans, titulaires d'au moins un baccalauréat. En outre, ce programme propose une formation informatique pratique, avec des compétences techniques en cybersécurité.
   https://cybersecuritymag.africa/young-women-tech-programme-de-formation-gratuite-cybersecurite-pour-les-jeunes-filles-ghana

5. **Lomé au cœur de la protection des données personnelles : un Forum international attendu en juillet 2025**
   Lomé s'apprête à accueillir du 28 au 30 juillet 2025, la première édition du Forum International sur la Protection des Données à Caractère Personnel au Togo (FIPDCP-Togo). Cette initiative d'envergure va positionner le Togo comme l'un des acteurs clés de la gouvernance numérique sur des questions de protection des données en Afrique. Ce rendez-vous réunira des experts internationaux, des acteurs locaux et des décideurs politiques pour débattre autour de la protection des données personnelles. Avec ce Forum, les organisateurs entendent sensibiliser, partager des expériences et proposer des solutions adaptées aux réalités africaines.
   https://cybersecuritymag.africa/lome-accueille-du-28-au-30-juillet-2025-premiere-edition-fipdcp-togo

6. **Faux CAPTCHAs et nouvelles techniques pour échapper à la détection**
   La dernière Au cours de ce mois de janvier, le Threat Labs de Netskope a signalé une nouvelle campagne de logiciels malveillants, utilisant de faux CAPTCHA afin de diffuser le malware Lumma Stealer, qui existe depuis 2022 et fonctionne comme un malware-as-a-service. La campagne a un impact à l'échelle mondiale : les experts de Netskope ont identifié des victimes en Argentine, en Colombie, aux États-Unis, et aux Philippines, entre autres. En outre, de nombreux secteurs sont touchés comme ceux de la santé, de la banque et du marketing. Par ailleurs, le secteur des télécommunications est celui qui compte le plus grand nombre d'organisations ciblées.

   https://www.undernews.fr/malwares-virus-antivirus/faux-captchas-et-nouvelles-techniques-pour-echapper-a-la-detection.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**.