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 Mai 2026

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 Google Chrome 5
Vulnérabilité dans Mozilla Firefox 6
II.2 SYSTÈMES D'EXPLOITATION 7
Vulnérabilité dans le noyau Linux de SUSE 7
Vulnérabilité dans le noyau Linux de Red Hat 7
Vulnérabilité dans le noyau Linux d'Ubuntu 8
Vulnérabilité dans le noyau Linux de Debian 8
Vulnérabilité dans Microsoft Windows 9
II.3 CMS 10
Vulnérabilité dans SPIP 10
Vulnérabilité dans Joomla ! 10
Vulnérabilité dans Drupal 11
II.4 AUTRES 12
Vulnérabilité dans les produits Microsoft 12
Vulnérabilité dans Microsoft Azure 12
Vulnérabilité dans Kaspersky Anti Targeted Attack Platform 13
Vulnérabilité dans Oracle Database Server 13

Vulnérabilité dans Elastic Kibana 13
Vulnérabilité dans Centreon Web 14
Vulnérabilité dans les produits Veeam 14
Vulnérabilité dans Symfony 15
Vulnérabilité dans Samba 16
Vulnérabilité dans les produits Check Point 16
Vulnérabilité dans Roundcube 17
Vulnérabilité dans Nginx 17
II.1 ACTUALITES 18
III. NOTES IMPORTANTES 20

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 148.0.3967.83	22/05/2026	CVE-2026-9126	148.0.3967.83 Télécharger	Mettre à jour le navigateur	8.8
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 148.0.7778.215 pour Linux • Chrome versions antérieures à 148.0.7778.216 pour Windows • Chrome versions antérieures à 148.0.7778.217 pour Mac	28/05/2026		148.0.7778.216 Télécharger	Mettre à jour le navigateur	

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Mozilla Firefox	Une vulnérabilité a été découverte dans Firefox pour iOS. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • Firefox pour iOS versions antérieures à 151.1	26/05/2026	CVE-2026-9078	151.1 Télécharger	Mettre à jour le navigateur	5.4

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 une atteinte à l'intégrité des données.	29/05/2026	CVE-2026-46333	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20262068-1	7.1
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 élévation de privilèges, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données.	29/05/2026	CVE-2026-43190	10.2 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:21745	8.2

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, un déni de service à distance et une atteinte à la confidentialité 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	29/05/2026	CVE-2026-43276	26.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8310-1	7.8
Vulnérabilité dans le noyau Linux de Debian	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Les versions affectées sont les suivantes : • Debian bookworm versions antérieures à 6.1.174-1 • Debian trixie versions antérieures à 6.12.90-2	29/05/2026	CVE-2026-46300	13.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00217.html	7.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Elles permettent à un attaquant de provoquer une élévation de privilèges et un contournement de la politique de sécurité. Microsoft indique qu'une preuve de concept est disponible publiquement pour la vulnérabilité CVE-2026-45585, aussi appelée YellowKey. À défaut de publier un correctif de sécurité, l'éditeur propose une mesure de contournement dans l'avis de sécurité associé (cf. section Documentation). Les systèmes affectés sont les suivants : • Windows 11 Version 24H2 pour systèmes x64 • Windows 11 Version 25H2 pour systèmes x64 • Windows 11 version 26H1 pour systèmes x64 • Windows Admin Center in Azure Portal versions antérieures à 0.72.0.0. • Windows Server 2025 • Windows Server 2025 (Server Core installation)	20/05/2026	CVE-2026-45585	11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585	6.8

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. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les versions affectées sont les suivantes : • SPIP versions antérieures à 4.4.15	22/05/2026		4.4.15 Télécharger	Mettre à jour le CMS	
Vulnérabilité dans Joomla !	De multiples vulnérabilités ont été découvertes dans Joomla! Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Joomla! versions 6.x antérieures à 6.1.1 • Joomla! versions antérieures à 5.4.6	27/05/2026	CVE-2026-48905	6.1.1 Télécharger	Mettre à jour le CMS	6.1

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 SQL (SQLi). L'éditeur précise que la vulnérabilité CVE-2026-9082 affecte uniquement les applications qui utilisent PostgreSQL comme système de gestion de base de données. Cependant, il recommande néanmoins l'installation du correctif pour toutes les instances du fait des mises à jour de dépendances également incluses dans les dernières versions.Les versions affectées sont les suivantes : • Drupal versions 11.3.x antérieures à 11.3.10 L'éditeur rappelle que les versions 11.1.x, 11.0.x, 10.4.x, 9.x et 8.x sont en fin de vie et ne reçoivent un correctif pour la vulnérabilité CVE-2026-9082 qu'à titre exceptionnel, au vu de sa criticité. Ces versions n'incluent pas de correctif pour toutes les autres vulnérabilités découvertes depuis leurs fins de support respectives. L'éditeur invite donc à migrer vers une version supportée et à jour.	21/05/2026	CVE-2026-9082	11.3.11 Télécharger	Mettre à jour le CMS	9.8

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 un problème de sécurité non spécifié par l'éditeur.	01/06/2026	CVE-2026-46598	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8466	5.3
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 1.4.0-1	01/06/2026	CVE-2026-39824	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-39824	3.3

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Kaspersky Anti Targeted Attack Platform	Une vulnérabilité a été découverte dans Kaspersky Anti Targeted Attack Platform. Elle permet à un attaquant de provoquer un déni de service à distance. Les systèmes affectés sont les suivants : • Anti Targeted Attack Server versions 8.0.x antérieures à 8.0.1	01/06/2026	CVE-2026-31932	8.0.1 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.kaspersky.com/vulnerability/list-of-advisories/12430#290526	7.5
Vulnérabilité dans Oracle Database Server	De multiples vulnérabilités ont été découvertes dans Oracle Database Server. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance. Les systèmes affectés sont les suivants : • Oracle Database Server (Net Service) versions 23.4.0 à 23.26.2	29/05/2026	CVE-2026-46835	23.26.02 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.oracle.com/security-alerts/cspumay2026.html	7.5
Vulnérabilité dans Elastic Kibana	De multiples vulnérabilités ont été découvertes dans Elastic Kibana. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, un déni de service à distance	29/05/2026	CVE-2026-49095	9.4.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://discuss.elastic.co/t/kibana-9-3-3-security-update-	6.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Kibana versions 8.x antérieures à 8.19.16 • Kibana versions 9.4.x antérieures à 9.4.2 • Kibana versions 9.x antérieures à 9.3.5				esa-2026-40/386562	
Vulnérabilité dans Centreon Web	De multiples vulnérabilités ont été découvertes dans Centreon Web. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Web versions 25.10.x antérieures à 25.10.12 • Web versions antérieures à 24.10.25	29/05/2026		24.10.25 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://thewatch.centreon.com/latest-security-bulletins-64/may-2026-monthly-security-bulletin-for-centreon-infra-monitoring-medium-5715	
Vulnérabilité dans les produits Veeam	De multiples vulnérabilités ont été découvertes dans les produits Veeam. Elles permettent à un attaquant de provoquer une exécution de code	28/05/2026	CVE-2026-32998	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.veeam	9.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	arbitraire à distance et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • ONE versions antérieures à 13.0.2.6723 • Service Provider Console versions 9.2.1.x antérieures à 9.2.1.33875 • Service Provider Console versions antérieures à 9.2.0.33215				.com/kb4858	
Vulnérabilité dans Symfony	De multiples vulnérabilités ont été découvertes dans Symfony. Certaines d'entre elles permettent à un attaquant de provoquer une falsification de requêtes côté serveur (SSRF), une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Symfony versions 7.0.x antérieures à 7.4.13 • Symfony versions 8.0.x antérieures à 8.0.13	27/05/2026	CVE-2025-48784	8.0.13 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://github.com/symfony/symfony/security/advisories/GHSA-x5qj-865h-mgvm	R

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Samba	De multiples vulnérabilités ont été découvertes dans Samba. 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. Les systèmes affectés sont les suivants : • Samba versions 4.23.x antérieures à 4.23.8 • Samba versions 4.24.x antérieures à 4.24.3 • Samba versions antérieures à 4.22.10	27/05/2026	CVE-2026-4480	4.24.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.samba.org/samba/security/CVE-2026-4480.html	8.5
Vulnérabilité dans les produits Check Point	De multiples vulnérabilités ont été découvertes dans les produits Check Point. 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 : • Security Gateways versions R82.10 sans le correctif 19 • Security Gateways versions R82.10 sans le correctif 19	27/05/2026	CVE-2026-48136	R82.10 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.checkpoint.com/results/sk/sk184993	4.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Roundcube	De multiples vulnérabilités ont été découvertes dans Roundcube. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Roundcube Webmail versions 1.6.x antérieures à 1.6.16 • Roundcube Webmail versions 1.7.x antérieures à 1.7.1	26/05/2026		1.7.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://roundcube.net/news/2026/05/24/security-updates-1.6.16-and-1.7.1	
Vulnérabilité dans Nginx	Une vulnérabilité a été découverte dans Nginx. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance et un déni de service à distance. Les systèmes affectés sont les suivants : • NGINX Plus versions 37.x antérieures à 37.0.1.1 • NGINX Plus versions Rx antérieures à R36 P5 ou R32 P7 L'éditeur indique que les versions 0.x de Nginx Open Source n'auront pas de correctifs	26/05/2026	CVE-2026-9256	R37 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://my.f5.com/manage/s/article/K000161377	9.2

II.1 ACTUALITES

1. **Cybersécurité et vie privée au Nigéria : la NDPC mobilise des administrations fédérales autour de la protection des données**
   Les autorités en charge de la protection des données personnelles au Nigéria ont inauguré ce lundi 1er juin 2026, la première session de formation aux Technical and Organisational Measures (TOMs) Drill on Data Protection Measures destinée aux administrateurs informatiques des ministères, départements et agences du gouvernement fédéral. Cette formation vise à faire face aux cyberattaques contre les infrastructures numériques gouvernementales. Ladite initiative vient soutenir le cadre du plan du gouvernement fédéral en vue de numériser intégralement ses opérations.
   https://cybersecuritymag.africa/ndpc-mobilise-des-administrations-federales-autour-de-la-protection-des-donnees/

2. **Le Bénin distingué lors des Cyber Games & Digital Security Challenge à Marrakech**
   Le Bénin s'est classé parmi les meilleurs participants de la deuxième édition des Cyber Games & Digital Security Challenge, organisée du 19 au 21 mai 2026 au Maroc. L'événement, porté conjointement par le Bureau du Programme de Lutte contre la Cybercriminalité du Conseil de l'Europe et la Direction de la Cybercriminalité d'Interpol, a réuni 160 participants venus de plus de 50 pays autour d'exercices et de défis consacrés à la sécurité numérique et à la lutte contre la cybercriminalité.
   https://cybersecuritymag.africa/le-benin-distingue-lors-des-cyber-games-digital-security-challenge-a-marrakech/

3. **Protection des systèmes d'information : l'ASSI Algérie réunit des cadres en formation spécialisée à l'ENSCS**
   L'Agence de la sécurité des systèmes d'information (ASSI-Algérie) a lancé ce 1er juin 2026 à l'École nationale supérieure de cybersécurité (ENSCS) de Sidi Abdellah à Alger, une session de formation de trois jours. Cette session de formation destinée aux cadres des institutions publiques et organismes nationaux vise à renforcer leurs compétences techniques. Aussi, selon l'ASSI, elle permet d'introduire les meilleures règles et normes pour l'application des bonnes pratiques en matière de cybersécurité lors des phases de développement des logiciels. Par ailleurs, ladite formation vient renforcer la capacité des cadres en matière des législations et réglementations relatives à la cybersécurité en Algérie.
   https://cybersecuritymag.africa/protection-des-systemes-information-assi-algerie-reunit-des-cadres-en-formation-specialisee/

4. **L'ANCS Tunisie alerte sur la hausse des risques liés à l'utilisation des réseaux sociaux**
   Les réseaux sociaux ne sont plus seulement des espaces d'échange et de communication. En **Tunisie**, ils sont désormais considérés par les autorités comme des vecteurs de risques sécuritaires en pleine expansion, à mesure que les cybercriminels exploitent les avancées de l'intelligence artificielle pour affiner leurs méthodes. Dans un avertissement rendu public par l'**Agence Nationale de la Cybersécurité (ANCS)**, les autorités signalent une recrudescence des cyberattaques qui ciblent les utilisateurs des plateformes numériques. Les menaces identifiées concernent notamment l'usurpation d'identité, la désinformation, le vol de données personnelles ainsi que des tentatives d'escroquerie de plus en plus élaborées. Cette situation est liée à un environnement technologique en mutation, où les outils liés à l'intelligence artificielle facilitent la création de contenus frauduleux difficiles à détecter. Les cybercriminels exploitent ces technologies pour produire des messages crédibles, imiter des styles d'écriture ou encore générer des contenus audiovisuels trompeurs.
   https://cybersecuritymag.africa/ancs-tunisie-alerte-sur-la-hausse-des-risques-lies-a-lutilisation-des-reseaux-sociaux/

5. **Le Ministère de l'Agriculture de la Tunisie impose l'installation d'un antivirus sur l'ensemble de ses postes informatiques**
   Confronté à des cybermenaces visant les infrastructures publiques, le Ministère de l'Agriculture, des Ressources hydrauliques et de la Pêche de la Tunisie a ordonné l'installation et l'activation d'un logiciel antivirus sur l'ensemble des postes informatiques de ses administrations centrales. La mesure s'accompagne d'une interdiction stricte de désactiver cet outil de protection. La décision a été formalisée dans une circulaire adressée le 25 mai 2026 aux directeurs généraux. Le document fixe des consignes strictes en matière de protection numérique et rend obligatoire l'équipement de tous les postes de travail concernés.
   https://cybersecuritymag.africa/ministere-de-lagriculture-de-tunisie-impose-installation-dun-antivirus-sur-lensemble-de-ses-postes-informatiques/

6. **Arnaques aux concours publics en Côte d'Ivoire : plus de 120 victimes et un préjudice estimé à 74 millions FCFA**
   En Côte d'Ivoire, une nouvelle vague d'escroqueries vise les chercheurs d'emploi à des postes administratifs. Récemment plusieurs personnes disent avoir reçu des messages et courriels frauduleux annonçant de prétendus recrutements dans des secteurs comme les impôts, les douanes ou encore le corps des attachés administratifs. Selon les témoignages recueillis, ces messages imitent des documents officiels : logos administratifs, faux cachets et convocations soigneusement falsifiées. Les cybercriminels exigeraient des frais de dossier allant de quelques centaines de milliers à plus d'un million de francs CFA pour garantir une place dans les concours.
   https://cybersecuritymag.africa/arnaques-aux-concours-publics-en-cote-divoire-plus-de-120-victimes/

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**.