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°1 du mois de Juillet 2026

B.P. 6170 Tél : 694 405 868 Web : https://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 une exécution de code arbitraire à distance, une élévation de privilèges et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Microsoft Edge versions antérieures à 150.0.4078.48	15/07/2026	CVE-2026-58596	150.0.4078.48 Télécharger	Mettre à jour le navigateur	8.3
Vulnérabilité dans Mozilla Firefox	De multiples vulnérabilités ont été découvertes dans Mozilla Firefox. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les versions affectées sont les suivantes : • Firefox versions antérieures à 152.0.6 • Firefox versions antérieures à 152.4 pour iOS	15/07/2026	CVE-2026-15719	152.0.6 Télécharger	Mettre à jour le navigateur	5.4

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, dont un use-after-free dans le composant Aura. Elles permettent à un attaquant de provoquer une corruption de la mémoire et une exécution de code arbitraire. Les versions affectées sont les suivantes : • Chrome versions antérieures à 150.0.7871.128 pour Windows et Linux • Chrome versions antérieures à 150.0.7871.129 pour Mac	17/07/2026	CVE-2026-15905	150.0.7871.128 Télécharger	Mettre à jour le navigateur	Non attribué (Élevée)

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, un déni de service à distance et une atteinte à la confidentialité des données.	17/07/2026	CVE-2026-53362	16.0 Essayer	Veuillez-vous référer au Bulletin de sécurité : https://www.suse.com/support/update/announcement/2026/suse-su-20263083-1	7.8
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.	17/07/2026	CVE-2026-53359	10.2 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:41229	8.8

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, un déni de service à distance et une atteinte à la confidentialité des données. Les versions affectées sont les suivantes : • Ubuntu 14.04 ESM • Ubuntu 16.04 ESM • Ubuntu 20.04 ESM • Ubuntu 24.04 LTS • Ubuntu 25.10	17/07/2026	CVE-2026-46325	26.04 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://ubuntu.com/security/notices/USN-8548-1	9.8
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 : aucun correctif publié à ce jour (statut « vulnérable » selon le suivi de sécurité Debian) • Debian trixie versions antérieures à 6.12.95-1	10/07/2026	CVE-2026-53362	13.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00292.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. 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.	17/07/2026	CVE-2026-59117	11 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-59117	7.5
Vulnérabilité dans Cisco RoomOS	De multiples vulnérabilités ont été découvertes dans Cisco RoomOS. 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 versions affectées sont les suivantes : • RoomOS versions 11 antérieures à 11.32.6.0 • RoomOS versions 26 antérieures à 26.5.2.2	16/07/2026	CVE-2026-20187	26.7.1.7 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-roomos-AqNMbEq	7.5

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 intersite (XSS) via un nettoyage insuffisant des libellés de blocs dans l'éditeur Layout Builder. L'exploitation nécessite que l'attaquant et l'utilisateur ciblé utilisent tous deux l'interface d'édition Layout Builder. Les versions affectées sont les suivantes : • Drupal versions 11.4.x antérieures à 11.4.4 • Drupal versions 11.3.x antérieures à 11.3.14 • Drupal versions 11.0.x, 11.1.x et 11.2.x (toutes versions. Branches non maintenues) • Drupal versions antérieures à 10.6.13	16/07/2026	CVE-2026-55805	11.4.4 Télécharger	Mettre à jour le CMS	13/25 (Modérément critique)

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Joomla !	De multiples vulnérabilités ont été découvertes dans Joomla!. 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 une injection de code indirecte à distance (XSS). Les versions affectées sont les suivantes : • Joomla! versions 6.x antérieures à 6.1.2 • Joomla! versions antérieures à 5.4.7	08/07/2026	CVE-2026-48958	6.1.2 Télécharger	Mettre à jour le CMS	8.8

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 une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Microsoft SharePoint Enterprise Server 2016 versions antérieures à 16.0.5561.1001 • Microsoft SharePoint Server 2019 versions antérieures à 16.0.10417.20175 • Microsoft SharePoint Server Subscription Edition versions antérieures à 16.0.19725.20434 • Remote Desktop Web Client versions antérieures à 2.1.65.2	17/07/2026	CVE-2026-62826	Explorer	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62826	4.6

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans les produits ESET	Une vulnérabilité a été découverte dans les produits ESET. Elle permet à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : • Endpoint Antivirus versions 13.2.x antérieures à 13.2.3.0	16/07/2026	CVE-2026-6424	13.2.3.0 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support-feed.eset.com/link/15370/17380664/ca8972	6.7
Vulnérabilité dans les produits SPLUNK	De multiples vulnérabilités ont été découvertes dans les produits Splunk. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une atteinte à l'intégrité des données, une injection de requêtes illégitimes par rebond (CSRF) et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Splunk Cloud Platform versions antérieures à 10.5.2605.0 (selon la branche : 10.1.2507.24 / 10.2.2510.18 / 10.3.2512.16 / 10.4.2604.7 / 10.5.2605.0) • Splunk Enterprise versions antérieures à 10.4.1 (selon la branche : 9.3.14 / 9.4.13 / 10.0.8 / 10.2.5 / 10.4.1)	16/07/2026	CVE-2026-8202 CVE-2026-8053	Variable selon le produit. Voir versions ci-contre Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.cert.ssi.gouv.fr/avis/CERTFR-2026-AVI-0888	6.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• Splunk Universal Forwarder versions antérieures à 10.4.1 (selon la branche : 9.4.13 / 10.0.8 / 10.2.5 / 10.4.1)					
Vulnérabilité dans Tenable Nessus Agent	Une vulnérabilité a été découverte dans Tenable Nessus Agent. Elle permet 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 : • Nessus Agent versions 11.2.x antérieures à 11.2.1	15/07/2026	CVE-2026-15265	11.2.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2026-18	9.1
Vulnérabilité dans les produits Citrix	De multiples vulnérabilités ont été découvertes dans les produits Citrix, couvrant deux bulletins distincts. CTX696734 (CVE-2026-53565 et CVE-2026-53566) permet à un attaquant local standard de provoquer une élévation de privilèges et une atteinte à la confidentialité des données sur le Secure Access Client et l'Endpoint Analysis Client. CTX696811 (CVE-2026-42491) permet à un attaquant du réseau de management, interceptant certaines	15/07/2026	CVE-2026-53566, CVE-2026-53565, CVE-2026-42491	26.6.1.20 / 26.5.1.7 / 2026.4.0 / 26.15.0 (selon le produit) Explorer	Veuillez-vous référer au Bulletin de sécurité : https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696734&articleURL=Citrix_Secure_Access_Client_for_Windows_and_Citrix_Endpoint_Analysis_Client_for_	8.5 / 6.8

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	requêtes HTTPS, d'agir avec les privilèges de l'administrateur intercepté sur XenCenter et son SDK. Les systèmes affectés sont les suivants : • Endpoint Analysis Client versions antérieures à 26.5.1.7 pour Windows (CVE-2026-53565 uniquement) • Secure Access Client versions antérieures à 26.6.1.20 pour Windows (CVE-2026-53565 et CVE-2026-53566) • XenCenter SDK client versions antérieures à 26.15.0 pour PowerShell et C# (CVE-2026-42491) • XenCenter versions antérieures à 2026.4.0 (CVE-2026-42491)				Windows_Security_Bulletin_for_CVE_2026_53565_and_CVE_2026_53566 Et pour XenCenter/XenCenter SDK (CVE-2026-42491) : https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696811&articleURL=XenServer_Security_Update_for_CVE_2026_42491	
Vulnérabilité dans Apache Tomcat	De multiples vulnérabilités ont été découvertes dans Apache Tomcat. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants :	15/07/2026	CVE-2026-59084	11.0.24 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.24	9.1

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• Tomcat versions 11.0.x antérieures à 11.0.24					
Vulnérabilité dans Microsoft Azure Linux	De multiples vulnérabilités ont été découvertes dans Microsoft Azure Linux. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • azl3 erlang 26.2.5.21-2 versions antérieures à 26.2.5.21-3	15/07/2026	CVE-2026-9079	Mettre à jour	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-59890	9.8
Vulnérabilité 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, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • FortiAuthenticator versions 6.6.x antérieures à 6.6.3 • FortiClientEMS antérieures à 7.4.6	15/07/2026	CVE-2026-59841	8.0 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-26-155	7.5

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	• FortiOS versions antérieures à 7.6.7 • FortiPAM versions 1.8.x antérieures à 1.8.3 • FortiProxy versions antérieures à 7.6.6 • FortiSandbox versions 5.0.x antérieures à 5.0.3 • FortiSIEM versions 7.4.x antérieures à 7.4.1 • FortiSIEMWindowsAgent versions 7.4.x antérieures à 7.4.2					
Vulnérabilité dans Veeam Backup & Replication	Une vulnérabilité a été découverte dans le composant Veeam Updater de Veeam Backup & Replication. Elle permet à un utilisateur local de provoquer une élévation de privilèges et d'obtenir un accès root sur le système d'exploitation sous-jacent. Cette faille ne concerne que les déploiements Linux (Veeam Software Appliance et Veeam Infrastructure Appliance) ; les serveurs VBR sous Windows ne sont pas affectés. Les systèmes affectés sont les suivants : • Composant Veeam Updater versions antérieures à 12.3.0.65	15/07/2026	CVE non attribué à ce jour (signalement via HackerOne)	13.0.2.29 (VBR global) correctif du composant Updater : 12.3.0.65 Explorer	Veuillez-vous référer au Bulletin de sécurité : https://www.veeam.com/kb4879	8.4

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Suricata	De multiples vulnérabilités ont été découvertes dans Suricata. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Suricata versions 8.x antérieures à 8.0.6	10/07/2026	CVE-2026-57229	8.0.6 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://suricata.io/2026/07/09/suricata-8-0-6-and-7-0-17-released/	N/A
Vulnérabilité dans Cpython	Une vulnérabilité a été découverte dans CPython. Elle permet à un attaquant de provoquer un déni de service à distance via l'analyseur HTML incrémental (html.parser.HTMLParser), en soumettant des déclarations de balisage non terminées et répétées. Les systèmes affectés sont les suivants : • CPython versions 3.9.x à 3.14.x (toutes versions antérieures à 3.15.0) • Correctif amont fusionné le 4 juillet 2026, mais non encore intégré dans une version officielle publiée à la date de ce bulletin. suivre les prochaines versions de maintenance de	10/07/2026	CVE-2026-15308	Aucune version corrigée publiée à ce jour. surveiller les prochaines mises à jour par branche Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/F6453LWKSHKCTWFLCOURWPLETNUIW2Z5/	8.7

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
	chaque branche (3.12.x, 3.13.x, 3.14.x) ou appliquer les rétroportages distributeur (Red Hat, AlmaLinux, etc.)					

III. ACTUALITES

1. **Le Togo et le Luxembourg signent un accord de coopération pour le programme de cybersécurité TogoCyber+**
   Le Togo et le Luxembourg ont signé, mercredi 15 juillet 2026 à Lomé, trois accords destinés à renforcer leur coopération bilatérale. Les textes portent sur le financement du programme environnemental INCLURE, le Programme indicatif de coopération (PIC) 2026-2031 et le lancement de TogoCyber+, un programme consacré au renforcement des capacités du pays en matière de cybersécurité. Les accords ont été paraphés par le Ministre des Affaires étrangères du Togo, Robert Dussey, et le Vice-Premier Ministre du Luxembourg, Xavier Bettel, en présence de la Ministre de l'Économie Numérique et de la Transformation digitale, Cina Lawson.
   https://cybersecuritymag.africa/le-togo-et-le-luxembourg-signent-un-accord-pour-le-programme-togocyber/

2. **L'Ouganda dévoile un nouveau cadre national pour renforcer la cybersécurité**
   Le Ministre des Technologies de l'Information et de la Communication et de l'Orientation Nationale de l'Ouganda, Justine Kasule Lumumba, a lancé le Cadre National de Sécurité de l'Information (NISF) mis à jour pour 2026. Ce document fournit aux institutions publiques des orientations pratiques, des outils d'évaluation de la cybersécurité ainsi que des exigences minimales de sécurité pour améliorer leur niveau de protection face aux menaces numériques. Lors du lancement, la Ministre a rappelé que la sécurité de l'information dépasse désormais les enjeux techniques et constitue un élément lié à la sécurité nationale, au développement économique, à la continuité des services publics et à la confiance des citoyens.
   https://cybersecuritymag.africa/ouganda-devoile-un-nouveau-cadre-national-pour-renforcer-la-cybersecurite/

3. **L'État algérien donne un mois aux administrations pour achever leur interconnexion au Data Center national**
   Le Président de l'Algérie a accordé aux administrations publiques un délai d'un mois pour raccorder leurs systèmes d'information au Centre National des données (Data Center). L'instruction a été annoncée lors du Conseil des Ministres du 12 juillet 2026 afin d'accélérer la numérisation des services publics et de renforcer les échanges de données entre les institutions de l'État. Cette interconnexion doit permettre aux administrations de partager automatiquement certaines informations, ce qui réduira les demandes répétées de documents auprès des citoyens. Elle doit également soutenir le déploiement du portail national « Dzair Digital Services », conçu pour faciliter les démarches administratives et développer les services publics en ligne.
   https://cybersecuritymag.africa/etat-algerien-donne-un-mois-aux-administrations-pour-achever-leur-interconnexion-au-data-center/

4. **Protection des enfants en ligne : le Zimbabwe adopte un cadre national**
   Le Zimbabwe a lancé la Politique Nationale de Protection des Enfants en Ligne IV (2026-2030) lors de la Conférence nationale sur la protection de l'enfance organisée à Bulawayo du 07 au 10 juillet 2026. Présentée conjointement avec le 4e Plan d'action national pour l'enfance (2026-2030), cette initiative établit un cadre destiné à lutter contre les risques liés à l'usage du numérique par les plus jeunes, notamment le cyberharcèlement, l'exploitation en ligne, le grooming numérique, la sextorsion et les atteintes à la vie privée. Selon le Ministère des Technologies de l'Information et de la Communication, la politique repose sur une approche coordonnée impliquant les pouvoirs publics, les entreprises privées, les établissements universitaires, la société civile et les communautés locales.
   https://cybersecuritymag.africa/protection-des-enfants-en-ligne-le-zimbabwe-adopte-un-cadre-national/

5. **Le Sénégal mobilise les acteurs publics et privés autour de la cybersécurité**
   Le Ministre des Télécommunications et du Numérique du Sénégal a présidé, le 13 juillet 2026, une réunion de concertation consacrée à la sécurité des systèmes d'information des infrastructures critiques. Organisée en présence de représentants de structures publiques et privées, la rencontre a porté sur le renforcement des dispositifs de cybersécurité, la coordination entre les acteurs concernés et les réponses à apporter à la multiplication des cybermenaces. L'objectif est d'anticiper l'entrée en vigueur du futur cadre réglementaire et de renforcer les dispositifs de prévention, de détection et de réaction face aux cyberattaques pouvant cibler des infrastructures critiques, dont une compromission pourrait provoquer d'importantes perturbations pour les citoyens et les services essentiels.
   https://cybersecuritymag.africa/senegal-mobilise-les-acteurs-publics-et-prives-autour-de-la-cybersecurite/

6. **La Tunisie réunit des acteurs africains autour de l'IA et de la sécurité numérique**
   La ville de Hammamet, en Tunisie, accueille du 13 au 15 juillet 2026 le Sommet africain de l'intelligence artificielle et de la cybersécurité. L'événement réunit des experts, des universitaires, des responsables publics, des décideurs et des acteurs du numérique venus échanger sur les enjeux de la gouvernance numérique, de l'intelligence artificielle et de la cybersécurité en Afrique. Les discussions portent notamment sur la protection des **infrastructures critiques**, le développement des compétences, la coopération scientifique et la mise en place de cadres communs pour la gouvernance des données et la sécurité numérique.
   https://cybersecuritymag.africa/tunisie-reunit-des-acteurs-africains-autour-de-ia-et-securite-numerique/

IV. NOTES IMPORTANTES

1. Veuillez enregistrer les adresses alerts@cirt.cm et alerts@cirt.antic.cm parmi vos contacts ou les enregistrer comme expéditeurs approuvés afin de ne plus recevoir les mails en provenance de ces adresses dans vos spams.
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 Linux 7 et CentOS Stream 8 ne sont plus supportés depuis, respectivement, le 30 juin 2024 et le 31 mai 2024. Si votre organisation n'a pas encore migré vers une version supportée, notamment CentOS Stream 9 ou 10 (voir https://www.centos.org/centos-stream/), votre système d'information court de grands risques. L'utilisation de solutions ne bénéficiant d'aucun support technique présente un risque élevé, étant donné qu'aucun correctif ne sera émis pour les vulnérabilités qui y seront découvertes.
4. Microsoft a mis fin au support de Windows 10 (toutes éditions grand public et professionnelles) depuis le 14 octobre 2025. Depuis cette date, les postes fonctionnant sous Windows 10 ne reçoivent plus les mises à jour de fonctionnalités ni les correctifs de sécurité, sauf souscription au programme payant de mises à jour étendues (ESU). Il est recommandé aux différents Organismes de planifier la migration de leurs postes utilisateurs vers Windows 11, en prenant en compte cette migration dans les prévisions budgétaires. Pour rappel, Windows 7 et Windows 8.1 ne sont plus supportés depuis, respectivement, le 14 janvier 2020 et le 10 janvier 2023.

   https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020
5. Afin de se prémunir au maximum d'éventuelles 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 compromis par des malwares 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'adresse email alerts@cirt.antic.cm ou au numéro de téléphone **8202**.