

REPUBLIQUE DU CAMEROUN

Paix - Travail - Patrie

**AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION
ET DE LA COMMUNICATION**

**Centre de Reponse Aux Incidents de Securite
Informatique**



REPUBLIC OF CAMEROON

Peace - Work - Fatherland

**NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION
TECHNOLOGIES**

Computer Incident Response Team

Bulletin N°2 du mois de Juillet 2026

Date de publication: 15/07/2026

Classification: Publique

Sommaire

I. Lexique du Bulletin	2
II. Vulnerabilites publiees	3
II.1 Navigateurs	3
II.2 Systemes d'exploitation	3
II.3 CMS	4
II.4 Autres	4
III. Actualites	6
IV. Notes importantes	7

I. Lexique du Bulletin

Expression	Signification
Date de publication	Date a laquelle la vulnerabilite a ete officiellement publiee par le developpeur ou constructeur
Derniere version	Derniere version
Description	Details sur la vulnerabilite, versions concernees, vecteur d'exploitation
Reference CVE	Reference CVE
Score CVSS	Common Vulnerability Scoring System - evaluation de 0 a 10
Solution	Correctif ou contournement recommande

II. Vulnérabilités publiées

II.1 Navigateurs

Vulnérabilité	Description	Date	CVE	Version	Solution	CVSS
Microsoft Edge	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized	03/07/2026	CVE-2026-58289	N/A	Appliquer les correctifs Microsoft (Windows Update)	9.0
Microsoft Edge	Improper authorization in Microsoft Edge (Chromium-based) allows an unauthorized attacker to bypass a security feature o	03/07/2026	CVE-2026-57983	N/A	Appliquer les correctifs Microsoft (Windows Update)	8.7
Microsoft Edge	External control of file name or path in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code	03/07/2026	CVE-2026-58293	N/A	Appliquer les correctifs Microsoft (Windows Update)	8.1
Microsoft Edge	Improper input validation in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a netw	03/07/2026	CVE-2026-57985	N/A	Appliquer les correctifs Microsoft	7.6
Microsoft Edge	Use after free in Microsoft Edge (Chromium-based) allows an unauthorized attacker to execute code over a network.	03/07/2026	CVE-2026-57984	N/A	Appliquer les correctifs Microsoft (Windows Update)	7.5
Microsoft Edge	Server-side request forgery (ssrf) in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofin	03/07/2026	CVE-2026-57993	N/A	Appliquer les correctifs Microsoft (Windows Update)	7.4
Microsoft Edge	Exposure of private personal information to an unauthorized actor in Microsoft Edge for Android allows an unauthorized a	03/07/2026	CVE-2026-58297	N/A	Appliquer les correctifs Microsoft (Windows Update)	7.1

II.2 Systèmes d'exploitation

Vulnérabilité	Description	Date	CVE	Version	Solution	CVSS
containerd	containerd is an open-source container runtime. Versions prior to 2.3.2, 2.2.5 and 2.1.9 contain a vulnerability in the	01/07/2026	CVE-2026-50195	2.3.2,	Mettre à jour containerd vers version corrigée	9.9
containerd	containerd is an open-source container runtime. In Versions prior to 2.3.2, 2.2.5 and 2.1.9, the CRI implementation impr	01/07/2026	CVE-2026-53492	2.3.2,	Mettre à jour containerd vers version corrigée	9.6
Produit concerné	In Trail of Bits ficking versions up to and including 0.1.11, the UnsafeImportsML analysis pass unconditionally calls A	04/07/2026	CVE-2026-14535	N/A	Appliquer les correctifs du fournisseur	8.8
containerd	containerd is an open-source container runtime. In versions prior to 1.7.33, 2.3.2, 2.2.5, 2.1.9, and 2.0.10 the CRI plu	01/07/2026	CVE-2026-53488	1.7.33,	Mettre à jour containerd vers version corrigée	8.8

Vulnérabilité	Description	Date	CVE	Version	Solution	CVSS
Esri Portal	A Weak Password Recovery Mechanism for Forgotten Password exists in Esri Portal for ArcGIS versions 12.1 and earlier on	07/07/2026	CVE-2026-13020	N/A	Appliquer les correctifs du fournisseur	8.1
gpsd	gpsd through release-3.27.5, fixed at commit 4c06658, contains a command injection vulnerability in gpsprof that allows	09/07/2026	CVE-2026-58459	release-3.27.5,	Appliquer les correctifs du fournisseur	7.8
containerd	containerd is an open-source container runtime. In versions prior to 1.7.32, 2.0.9, 2.2.4 and 2.3.1, containers launched	01/07/2026	CVE-2026-46680	1.7.32,	Mettre à jour containerd vers version corrigée	7.8
Produit concerné	A local privilege escalation vulnerability in the WatchGuard Mobile VPN with SSL client for Windows allows a local attack	03/07/2026	CVE-2026-13079	N/A	Appliquer les correctifs du fournisseur	7.8

II.3 CMS

Vulnérabilité	Description	Date	CVE	Version	Solution	CVSS
WordPress	Blocksy Companion Pro plugin for WordPress before 2.1.47 contains an unauthenticated arbitrary file upload vulnerability	08/07/2026	CVE-2026-58480	2.1.47	Mettre à jour le plugin WordPress vers la dernière version	9.8
Joomla	The Joomla extension RSFiles is vulnerable to an unauthenticated arbitrary file upload that allows uploading executable	11/07/2026	CVE-2026-57827	N/A	Mettre à jour l'extension Joomla vers la dernière version	9.8
Joomla	The Joomla extension Helix Ultimate is vulnerable to an unauthenticated arbitrary file deletion.	13/07/2026	CVE-2026-57830	N/A	Mettre à jour l'extension Joomla vers la dernière	9.1
Balbooa Forms	Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability	10/07/2026	CVE-2026-56291	N/A	Mettre à jour l'extension Joomla vers la dernière	0
iCagenda	iCagenda Unrestricted Upload of File with Dangerous Type Vulnerability	10/07/2026	CVE-2026-48939	N/A	Mettre à jour l'extension Joomla vers la dernière	0
JoomShaper SP Page Builder	JoomShaper SP Page Builder Unrestricted Upload of File with Dangerous Type Vulnerability	07/07/2026	CVE-2026-48908	N/A	Mettre à jour l'extension Joomla vers la dernière version	0

II.4 Autres

Vulnérabilité	Description	Date	CVE	Version	Solution	CVSS
Traefik	Traefik is an HTTP reverse proxy and load balancer. Prior to v2.11.51, v3.6.22, and v3.7.6, Traefik's BasicAuth, DigestA	06/07/2026	CVE-2026-54763	writing	Mettre à jour Traefik vers v2.11.51/v3.6.22+	10.0
Produit concerné	A malicious actor with access to the network and low privileges could exploit a Server-Side Request Forgery (SSRF) in Un	02/07/2026	CVE-2026-55115	N/A	Appliquer les correctifs du fournisseur	9.9

Vulnérabilité	Description	Date	CVE	Version	Solution	CVSS
BeyondTrust	A high-severity vulnerability exists in a web application component of BeyondTrust Remote Support and Privileged Remote	06/07/2026	CVE-2026-40141	N/A	Appliquer le correctif BeyondTrust	9.9
Produit concerné	An XML injection vulnerability in the Large Scale VPN (LSVPN) functionality of Palo Alto Networks PAN-OS® software enabl	09/07/2026	CVE-2026-0284	N/A	Appliquer les correctifs du fournisseur	9.9
Produit concerné	A malicious actor with access to the network and low privileges could exploit an Improper Input Validation vulnerability	02/07/2026	CVE-2026-54402	N/A	Appliquer les correctifs du fournisseur	9.9
Azure OpenAI	Server-side request forgery (ssrf) in Azure OpenAI allows an authorized attacker to elevate privileges over a network.	02/07/2026	CVE-2026-45499	N/A	Appliquer les correctifs Microsoft	9.9
Microsoft Entra	Server-side request forgery (ssrf) in Microsoft Entra Provisioning Service (SyncFabric) allows an authorized attacker to	02/07/2026	CVE-2026-57100	N/A	(Windows Update) Appliquer les correctifs Microsoft (Windows Update)	9.9
MediaWiki	Deserialization of untrusted data vulnerability in Wikimedia Foundation MediaWiki.	01/07/2026	CVE-2026-58025	N/A	Appliquer les correctifs du fournisseur	9.8
Produit concerné	This vulnerability is associated with JAIOTlink C492A-W6 Wi-Fi IP cameras running firmware 4.8.30.57701411 contain a hard-coded credentials vulnerability that	01/07/2026	CVE-2026-58453	N/A	Appliquer les correctifs du fournisseur	9.8
MediaWiki	Improper neutralization of special elements used in an SQL command ('SQL injection') vulnerability in The Wikimedia Foun	01/07/2026	CVE-2026-58521	1.43.9,1.4	Appliquer les correctifs du fournisseur	9.8

III. Actualites

Cameroon deploys cybersecurity system to protect DPI, boost digital trust - Biometric Update

<a href="https://news.google.com/rss/articles/CBMisAFBVV95cUxNXzJqbm5MVm9ZSIFwaXBZZ0hPZEZrRHFIRmF5dnYzZ1ZxWklWcDlkUWQ1Wi1FanFudGV4YW14R1BtVWILZU5lZFU1SjJJR01XRWNsdTd4aC1EQ0xqcUtySXREbXA2S3hsdXRDWw2MkxrenVYaGd4dWZjSmxfUk9BU0tWMGY4ZFZRT2V3VmJxS2RyWFBKQVJuMVlyZERWUkhPWTRvZE5tWVhsMExhX1daRg?oc=5" targe

Source: <https://news.google.com/rss/articles/CBMisAFBVV95cUxNXzJqbm5MVm9ZSIFwaXBZZ0hPZEZrRHFIRmF5dnYzZ1ZxWklWcDlkUWQ1Wi1FanFudGV4YW14R1BtVWILZU5lZFU1SjJJR01XRWNsdTd4aC1EQ0xqcUtySXREbXA2S3hsdXRDWw2MkxrenVYaGd4dWZjSmxfUk9BU0tWMGY4ZFZRT2V3VmJxS2RyWFBKQVJuMVlyZERWUkhPWTRvZE5tWVhsMExhX1daRg?oc=5> tar

Cameroon Strengthens Cybersecurity with Advanced Systems at National CIRT - TechAfrica News

<a href="https://news.google.com/rss/articles/CBMisgFBVV95cUxPMExfa0VGMEJ5cnlLNjEyVTRQYjdERHpkcFdDWi05aVg0QlhuSmNUUV9HcXJnY2VKUFJETnhBT0V4ZjJ2aWl6amdad0ZUNE9TNWl3dkFOdG9uaDFLODVPamx0M1piM1dnaWNtejhJTTFmdnpaRFJCajVhYVdLQ1Qxd0xlU0xiNUNYMjkkNmhQM0syd2pYa01iWEoxUmFRd2FPcXBqUmlXeFlwd2d0X1A4WHdn?oc=5" tar

Source: <https://news.google.com/rss/articles/CBMisgFBVV95cUxPMExfa0VGMEJ5cnlLNjEyVTRQYjdERHpkcFdDWi05aVg0QlhuSmNUUV9HcXJnY2VKUFJETnhBT0V4ZjJ2aWl6amdad0ZUNE9TNWl3dkFOdG9uaDFLODVPamx0M1piM1dnaWNtejhJTTFmdnpaRFJCajVhYVdLQ1Qxd0xlU0xiNUNYMjkkNmhQM0syd2pYa01iWEoxUmFRd2FPcXBqUmlXeFlwd2d0X1A4WHdn?oc=5> tar

Cameroon Eyes AI-Driven Future: As Minpostel Engages With Canada-Africa Tech Leaders - Cameroon-Tribune

<a href="https://news.google.com/rss/articles/CBMizwFBVV95cUxNN0FweVh4VklRWVhYkd5SkVvS3E3LUoyYVWVHskxCZkjrZ1FEWHZZMUR5aExsYkR1Unp4emlKa2Mza2FxUVVvc0szVWtoSWVTejVmtTThfcHZYbGoxVTVTVzIjBvVnBnUThoclBxOHdtOUdxMU9ELXCX09ON2ZsS3prWnBTRmVvTGpjS1EtcDgwQTNVcFIUZEIrc3F6VGFvUUxKeVNfVnR2TTVzbzc5Yzh3VkJzelowRWxGcV

Source: <https://news.google.com/rss/articles/CBMizwFBVV95cUxNN0FweVh4VklRWVhYkd5SkVvS3E3LUoyYVWVHskxCZkjrZ1FEWHZZMUR5aExsYkR1Unp4emlKa2Mza2FxUVVvc0szVWtoSWVTejVmtTThfcHZYbGoxVTVTVzIjBvVnBnUThoclBxOHdtOUdxMU9ELXCX09ON2ZsS3prWnBTRmVvTGpjS1EtcDgwQTNVcFIUZEIrc3F6VGFvUUxKeVNfVnR2TTVzbzc5Yzh3VkJzelowRWxGcV>

Cameroon 2025: explosion of cyberattacks according to ANTIC - Digital Business Africa

<a href="https://news.google.com/rss/articles/CBmi_AFBVV95cUxPeWnkZTVWadZzN2xkMnV0Z0JyejJVZnRaMFQtZndjVEIMOWc4VmtBOGtWR04zaXpmZHhsNEctRTlxN09yd3BNN0VITzJNTU01eTA5LWZjdUzdlUzd0RGaHdXZeh5bUR5VGk2ZGVzV2FRdUZRsdNY0FkTdlfQWY4S2ozYXd2alpqcZVkb6QTA4Q1IXZlJYYWZ6SFNISTFUUI2FIZZUFSb2IFZTBKZTJLNFFBTHdOU2RJT2

Source: https://news.google.com/rss/articles/CBmi_AFBVV95cUxPeWnkZTVWadZzN2xkMnV0Z0JyejJVZnRaMFQtZndjVEIMOWc4VmtBOGtWR04zaXpmZHhsNEctRTlxN09yd3BNN0VITzJNTU01eTA5LWZjdUzdlUzd0RGaHdXZeh5bUR5VGk2ZGVzV2FRdUZRsdNY0FkTdlfQWY4S2ozYXd2alpqcZVkb6QTA4Q1IXZlJYYWZ6SFNISTFUUI2FIZZUFSb2IFZTBKZTJLNFFBTHdOU2RJT2

Cameroon Steps Up Cybercrime Response as Attacks Surge With Digital Shift - StopBlaBlaCam

<a href="https://news.google.com/rss/articles/CBMiwvFBVV95cUxQS2k3T1dObEFfalJpYWhRNVE1MzU4QWV2UDZsZGstdm1pSTV5X1ZSWDFzM3NQSOZqRG9JbmRpR0RyWGXlcV96emFzNk1yQWFCOXB0QlJuOVNObkjqSFE1OWdRRnNadVBVeGRDeDNaMINIWEQ5bldvOEVBcW9HRk9iUW9vQ1htQ2dON3I3Mjg0SVJqSzVKR1RaYmdoTDQ1TFIVM1Z4aXV5STluMzhweS1YdGIDWEEdmc3NLNG

Source: <https://news.google.com/rss/articles/CBMiwvFBVV95cUxQS2k3T1dObEFfalJpYWhRNVE1MzU4QWV2UDZsZGstdm1pSTV5X1ZSWDFzM3NQSOZqRG9JbmRpR0RyWGXlcV96emFzNk1yQWFCOXB0QlJuOVNObkjqSFE1OWdRRnNadVBVeGRDeDNaMINIWEQ5bldvOEVBcW9HRk9iUW9vQ1htQ2dON3I3Mjg0SVJqSzVKR1RaYmdoTDQ1TFIVM1Z4aXV5STluMzhweS1YdGIDWEEdmc3NLNG>

IV. 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 7 n'est plus supporté depuis 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.
4. Microsoft a mis fin au support de Windows 7 depuis le 14 janvier 2020. Il est recommandé de planifier la migration des postes utilisateurs utilisant encore ce système.