REPUBLIC OF CAMEROON
Peace - Work - Fatherland
NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES
Computer Incident Response Team

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

Bulletin N°2 of July 2026

Publication date: 15/07/2026

Classification: Public

Summary

I. Bulletin Lexicon

Term	Definition
Date de publication	Date when the vulnerability was officially published by the developer or manufacturer
Latest version	Derniere version
Description	Details about the vulnerability, affected versions, exploitation vector
CVE Reference	Reference CVE
CVSS Score	Common Vulnerability Scoring System - rating from 0 to 10
Solution	Recommended patch or workaround

II. Published Vulnerabilities

II.1 Browsers

Vulnerability	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 (Windows Update)	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	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 Operating Systems

Vulnerability	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 a jour containerd vers version corrigee	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 a jour containerd vers version corrigee	9.6
Produit concerne	In Trail of Bits fickling 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 a jour containerd vers version corrigee	8.8

Vulnerability	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 a jour containerd vers version corrigee	7.8
Produit concerne	A local privilege escalation vulnerability in the WatchGuard Mobile VPN with SSL client for Windows allows a local attac	03/07/2026	CVE-2026-13079	N/A	Appliquer les correctifs du fournisseur	7.8

II.3 CMS

Vulnerability	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 a jour le plugin WordPress vers la derniere 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 a jour l'extension Joomla vers la derniere 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 a jour l'extension Joomla vers la derniere	9.1
Balbooa Forms	Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability	10/07/2026	CVE-2026-56291	N/A	Mettre a jour l'extension Joomla vers la derniere	0
iCagenda	iCagenda Unrestricted Upload of File with Dangerous Type Vulnerability	10/07/2026	CVE-2026-48939	N/A	Mettre a jour l'extension Joomla vers la derniere version	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 a jour l'extension Joomla vers la derniere version	0

II.4 Others

Vulnerability	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 a jour Traefik vers v2.11.51/v3.6.22+	10.0
Produit concerne	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

Vulnerability	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 concerne	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 concerne	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 (Windows Update)	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	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 concerne	This vulnerability is associated wi 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. News

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

<a
href="https://news.google.com/rss/articles/CBMisAFBVV95cUxNXzJqbm5MVm9ZSlFwaXBZZ0hPZEZrRHFiRmF5dnYzZ1ZxWklWcDlkUWQ1Wi1FanFudGV4YW14R1BtVWlLZU5lZFU1SjJJR01XRWNsdTd4aC1EQ0xqcUtySXREbXA2S3hsdXRDWWw2MkxrenVYaGd4dWZjSmxfUk9BUWtWMGY4ZFZRT2V3VmJxS2RyWFBKQVJuMVlyZERWUkhPWTRvZE5tWVhsMExhX1daRg?oc=5" targe

Source: https://news.google.com/rss/articles/CBMisAFBVV95cUxNXzJqbm5MVm9ZSlFwaXBZZ0hPZEZrRHFiRmF5dnYzZ1ZxWklWcDlkUWQ1Wi1FanFudGV4YW14R1BtVWlL

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

<a
href="https://news.google.com/rss/articles/CBMisgFBVV95cUxPMExfa0VGMEJ5cnlLNjEyVTRQYjdERHpkcFdDWi05aVg0QlhuSmNUUV9HcXJnY2VKUFJETnhBT0V4ZjJ2aWl6amdad0ZUNE9TNWl3dkFOdG9uaDFLODVPamx0M1piM1dnaWNtejhJTTFmdnpaRFJCajVhYVdLQ1Qxd0xlU0xINUNYMjkxNmhQM0syd2pYa01iWEoxUmFRd2FPcXBqUmlXeFlwd2d0X1A4WHdn?oc=5" tar

Source: https://news.google.com/rss/articles/CBMisgFBVV95cUxPMExfa0VGMEJ5cnlLNjEyVTRQYjdERHpkcFdDWi05aVg0QlhuSmNUUV9HcXJnY2VKUFJETnhBT0V4ZjJ2aWl

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

<a
href="https://news.google.com/rss/articles/CBMizwFBVV95cUxNN0FweVh4VkVLRWVhYkd5SkVvS3E3LUoyYWVHSkxCZkJrZ1FEWHZZMUR5aExsYkR1Unp4emlKa2Mza2FxUVVVc0szVWtoSWVTejVmTThfcHZYbGoxVTVTVzlBVVBnUThoclBxOHdtOUdxMU9ELXZCX09ON2ZsS3prWnBTRmVvTGpjS1EtcDgwQTNVcFlUZElrc3F6VGFvUUxKeVNfVnR2TTVzbzc5Yzh3VkFzelowRWxGcV

Source: https://news.google.com/rss/articles/CBMizwFBVV95cUxNN0FweVh4VkVLRWVhYkd5SkVvS3E3LUoyYWVHSkxCZkJrZ1FEWHZZMUR5aExsYkR1Unp4emlKa2Mza2Fx

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

<a
href="https://news.google.com/rss/articles/CBMi_AFBVV95cUxPeWNKZTVWaDZzN2xkMnV0Z0JyejJVZnRaMFQtZndjVElMOWc4VmtBOGtWR04zaXpmZHhsNEctRTlxN09yd3BNN0VlTzJNTU01eTA5LWZjdlUzd0RGaHdXZEh5bUR5VGk2ZGVzV2FRdUZrS2dNY0FkTDlfQWY4S2ozYXd2alpqczVkSTB6QTA4Q1lXZlJYYWZ6SFNlSTFUQUl2ZFlZZUFSb2lFZTBKZTJLNFFBTHdOU2RJT2

Source: https://news.google.com/rss/articles/CBMi_AFBVV95cUxPeWNKZTVWaDZzN2xkMnV0Z0JyejJVZnRaMFQtZndjVElMOWc4VmtBOGtWR04zaXpmZHhsNEctRTlxN09yd

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

<a
href="https://news.google.com/rss/articles/CBMivwFBVV95cUxQS2k3T1dObEFfalJpYWhRNVE1MzU4QWV2UDZsZGstdm1pSTV5X1ZSWDFzM3NQS0ZqRG9JbmRpR0RyWGxLcV96emFzNk1yQWFCOXB0QlJuOVNObkJqSFE1OWdRRnNadVBYeGRDeDNaMlNlWEQ5bldvOEVBcW9HRk9iUW9vQ1htQ2dON3l3Mjg0SVJqSzVKR1RaYmdoTDQ1TFlVM1Z4aXV5STluMzhweS1YdGlDWEdmc3NLNG

Source: https://news.google.com/rss/articles/CBMivwFBVV95cUxQS2k3T1dObEFfalJpYWhRNVE1MzU4QWV2UDZsZGstdm1pSTV5X1ZSWDFzM3NQS0ZqRG9JbmRpR0RyW

IV. Important Notes

1. Veuillez enregistrer les adresses alerts@cirt.cm et alerts@cirt.antic.cm parmi vos contacts ou l'enregistrer comme expediteur approuve afin de ne plus recevoir les mails en provenance de cette adresse dans vos spam.

2. Ce document est produit regulierement et telechargeable sur notre site web www.cirt.cm. Vous y trouverez aussi des alertes et autres publications relatives a la cybersecurite et a la cybercriminalite.

3. CentOS 7 n'est plus supporte depuis juin 2024. L'utilisation des solutions ne possedant aucun support technique presente un risque eleve etant donne qu'aucun correctif ne sera emis apres d'eventuelles vulnerabilites detectees.

4. Microsoft a mis fin au support de Windows 7 depuis le 14 janvier 2020. Il est recommande de planifier la migration des postes utilisateurs utilisant encore ce systeme.