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 Aout 2026

Date de publication: 15/08/2026

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 3

II.4 Autres 4

III. Actualites 5

IV. Notes importantes 6

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. Vulnerabilites publiees

II.1 Navigateurs

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Microsoft Edge (Chromium)	Access of resource using incompatible type ('type confusion') in Microsoft Edge (Chromium-based) allows an unauthorized	04/08/2026	CVE-2026-66321	Avant correctif Aout 2026	Mettre a jour Microsoft Edge	7.4
Microsoft Edge for Android	External control of file name or path in Microsoft Edge for Android allows an unauthorized attacker to disclose informat	04/08/2026	CVE-2026-66310	Avant correctif Aout 2026	Mettre a jour Microsoft Edge	7.7
Microsoft Edge (Chromium)	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Teams for Android allows an	11/08/2026	CVE-2026-65768	Avant correctif Aout 2026	Mettre a jour Microsoft Edge	8.8

II.2 Systemes d'exploitation

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Microsoft Windows AFD.sys	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges loca	11/08/2026	CVE-2026-68820	Versions concernees Windows	Appliquer les correctifs Microsoft (KEV)	7.0
IBM i 7.3 a 7.6	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to execute arbitrary code due to an uncontrolle	12/08/2026	CVE-2026-16860	7.3, 7.4, 7.5, 7.6	Appliquer les correctifs IBM	9.9
IBM i 7.3 a 7.6	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a remote authenticated attacker to escalate privileges due to improper authoriz	12/08/2026	CVE-2026-17276	7.3, 7.4, 7.5, 7.6	Appliquer les correctifs IBM	9.6
Cisco Secure Firewall ASA/FTD	A vulnerability in the Remote Access SSL VPN service for Cisco Secure Firewall Adaptive Security Appliance (ASA) Softwar	11/08/2026	CVE-2026-20349	Versions ASA concernees	Appliquer le correctif Cisco (KEV)	8.6

II.3 CMS

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
OpenEMR	OpenEMR through 8.2.0 contains a remote code execution vulnerability in the document category tree component (library/cl	03/08/2026	CVE-2026-39932	Jusqu'a 8.2.0	Mettre a jour OpenEMR	9.1
RapiSafe (plugin WordPress)	The RapiSafe - Secure Multi File Upload for Contact Form 7 plugin for WordPress is vulnerable to arbitrary file deletion	15/08/2026	CVE-2026-14484	Toutes versions	Desactiver ou mettre a jour le plugin	9.1
6Storage Rentals (plugin WordPress)	The 6Storage Rentals plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.27.	15/08/2026	CVE-2026-15303	Toutes versions	Mettre a jour le plugin	9.8
User Session Synchronizer (plugin WordPress)	The User Session Synchronizer plugin for WordPress is vulnerable to Authentication Bypass leading to Account Takeover in	15/08/2026	CVE-2026-15341	Toutes versions	Mettre a jour le plugin	9.8

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
User Profile Builder (plugin WordPress)	The User Profile Builder plugin for WordPress is vulnerable to Authentication Bypass via Type Confusion in versions up t	15/08/2026	CVE-2026-15826	Toutes versions	Mettre a jour le plugin	9.8
TrueBooker (plugin WordPress)	The TrueBooker plugin for WordPress is vulnerable to Account Takeover in all versions up to, and including, 1.2.6. This	15/08/2026	CVE-2026-16142	Toutes versions	Mettre a jour le plugin	9.8
Ninja Tables Pro (plugin WordPress)	Ninja Tables Pro 5.2.11 contains an embedded malicious code vulnerability introduced via a tampered plugin build served	13/08/2026	CVE-2026-73533	5.2.11	Mettre a jour le plugin	9.8
Grav plugin-api	The getgrav/grav-plugin-api plugin before 1.0.13 fails to validate that the scopes of a newly created API key are a subs	14/08/2026	CVE-2026-72826	Avant 1.0.13	Mettre a jour le plugin	9.8
SPIP	SPIP before 4.4.18 contains a code injection vulnerability in SQLite-backed installations. The navigation menu endpoint	10/08/2026	CVE-2026-66738	Avant 4.4.18	Mettre a jour SPIP	8.8

II.4 Autres

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
MindsDB Minds Platform	MindsDB Minds Platform version 26.1.0 and earlier contains an unauthenticated remote code execution vulnerability that a	14/08/2026	CVE-2026-73678	26.1.0 et anterieures	Mettre a jour MindsDB	10.0
Metabase	Metabase allows a remote, unauthenticated attacker to inject arbitrary SQL via the '/reset_password' database endpoint a	10/08/2026	CVE-2026-72898	Versions concernees	Appliquer le correctif Metabase (KEV)	10.0
Apache NiFi	Apache NiFI 1.10.0 through 2.10.0 provide a Parameter Context update REST API method that does not enforce authorization	03/08/2026	CVE-2026-68979	1.10.0 a 2.10.0	Mettre a jour Apache NiFi	9.8
D-Link DWR-M961	D-Link DWR-M961 devices with hardware version C1 and software version 1.1.2_C1_202602110044 contain a buffer overflow vu	08/08/2026	CVE-2026-71957	1.1.2_C1_20260211004	Mettre a jour le firmware	9.8
MSI Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the dmz function that al	09/08/2026	CVE-2026-71986	v781521	Mettre a jour le firmware	9.8
MSI Radix AXE6600	MSI Radix AXE6600 router firmware version v781521 contains a command injection vulnerability in the TelnetSSH function u	09/08/2026	CVE-2026-71991	v781521	Mettre a jour le firmware	9.8
Eclipse Jetty	In Eclipse Jetty, the Digest authentication server-side component uses ISO-8859-1 to encode the password as bytes. This	04/08/2026	CVE-2026-10050	Versions concernees	Mettre a jour Eclipse Jetty	9.1
IBM Db2 Mirror for i	IBM Db2 Mirror for i 7.4, 7.5, and 7.6 could allow a remote attacker to execute arbitrary code due to external control o	14/08/2026	CVE-2026-17184	7.4, 7.5, 7.6	Appliquer les correctifs IBM	9.8
N-able N-central	An incomplete patch for CVE-2026-18556 allows for authentication bypass and account takeover in N-central Versions throu	02/08/2026	CVE-2026-18577	Versions concernees	Appliquer le correctif N-able (KEV)	8.1

III. Actualites

Cameroun : le CIRT national se dote de systemes avances pour renforcer la cybersecurite

Le Cameroun renforce son dispositif national de cybersecurite avec le deploiement de systemes avances au sein du Centre de Reponse aux Incidents de Securite Informatique (CIRT). Cette modernisation vise a proteger l'infrastructure numerique du pays, a renforcer la confiance numerique et a repondre plus efficacement a la hausse des cyberattaques observee avec la transformation digitale. Le pays travaille egalement a atteindre 98% de validation DNSSEC sur l'ensemble de son internet national d'ici 2026.

Source: https://news.google.com/rss/articles/CBMisgFBVV95cUxPMExfa0VGMEJ5cnlLNjEyVTRQYjdERHpkcFdDWi05aVg0QlhuSmNUUV9Hc

INTERPOL alerte sur l'essor des cyberattaques en Afrique dopees a l'intelligence artificielle

INTERPOL tire la sonnette d'alarme face a la multiplication des cyberattaques en Afrique, desormais amplifiees et rendues plus sophistiquees par l'intelligence artificielle. Deepfakes, phishing et malwares sont de plus en plus deployes a grande echelle sur le continent, ciblant aussi bien les institutions publiques que les entreprises privees. L'organisation appelle les Etats africains a renforcer leurs capacites de detection et de reponse.

Source: https://news.google.com/rss/articles/CBMixwFBVV95cUxPWWR4M0FfRE5rOThKcEwxd3NVZWZfYkNIY0FfdkFOM1RnUWg3b1BSV000U

Cybercriminalite : les pertes en Afrique atteignent 5 milliards de dollars en 2025, alerte INTERPOL

Selon INTERPOL, les pertes liees a la cybercriminalite en Afrique ont atteint environ 5 milliards de dollars en 2025. Ce chiffre illustre l'ampleur de la menace qui pese sur le continent, ou la fraude financiere, les ransomwares et les campagnes de phishing se developpent rapidement. Les institutions financieres et les administrations publiques figurent parmi les cibles privilegiees des groupes criminels.

Source: https://news.google.com/rss/articles/CBMi0wFBVV95cUxOQ0FyeEFmcUxjQ3NINnBzRXRJWG1ZUXBaZkk1ckpwOWJjMFhTVXIxMVZFN

Gabon : la SEEG reprend le controle apres une cyberattaque massive

La Societe d'energie et d'eau du Gabon (SEEG) a repris le controle de ses systemes apres avoir ete victime d'une cyberattaque massive. L'incident a perturbe temporairement certains services et illustre la vulnerabilite croissante des operateurs d'infrastructures critiques en Afrique centrale. Les autorites gabonaises ont ouvert une enquete pour identifier les auteurs de l'attaque.

Source: https://news.google.com/rss/articles/CBMiogFBVV95cUxOeUFqX2tiS3NnZW1fZ0FTcEt4MURXYkFUSExpTk5MOVJObXVGdk8yY2tZO

IV. Notes importantes

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.