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°1 du mois de Septembre 2026

Date de publication: 01/09/2026

Classification: Publique

Sommaire

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
Mozilla Firefox	Use-after-free dans le composant JavaScript/WebAssembly de Firefox permettant l'execution de code arbitraire.	18/08/2026	CVE-2026-74936	154 / ESR 140.14	Mettre a jour Firefox vers la version 154 ou	9.8
Mozilla Firefox	Use-after-free dans le composant Graphics/Text de Firefox permettant l'execution de code arbitraire.	18/08/2026	CVE-2026-74940	154 / ESR 115.39	Mettre a jour Firefox vers la version 154 ou	9.8
Mozilla Firefox	Use-after-free dans le composant DOM Core & HTML de Firefox permettant l'execution de code arbitraire.	18/08/2026	CVE-2026-74944	154 / ESR 140.14	Mettre a jour Firefox vers la version 154 ou ESR 115.39	9.8
WebKitGTK	Corruption memoire lors du traitement de contenu web malveillant dans WebKitGTK permettant l'execution de code arbitrair	31/08/2026	CVE-2026-83596	Derniere version	Mettre a jour WebKitGTK vers la derniere version disponible	8.8

II.2 Systemes d'exploitation

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
IBM AIX 7.2 / 7.3, PowerVM VIOS 4.1	Execution de code arbitraire a distance due a un defaut de debordement de tas (heap-based) dans IBM AIX et PowerVM	20/08/2026	CVE-2026-17436	7.2 / 7.3 / VIOS 4.1	Appliquer les correctifs IBM APAR	8.8
IBM AIX 7.2 / 7.3, PowerVM VIOS 4.1	Execution de code arbitraire a distance due a une authentification inappropriee dans IBM AIX et PowerVM VIOS.	20/08/2026	CVE-2026-17000	7.2 / 7.3 / VIOS 4.1	Appliquer les correctifs IBM APAR recommandes	8.1
IBM AIX 7.2 / 7.3	Elevation de privileges dans IBM AIX permettant a un attaquant local d'obtenir les privileges root.	20/08/2026	CVE-2026-16927	7.2 / 7.3	Appliquer les correctifs IBM APAR	7.3
Sudo	Contournement des politiques d'interception ptrace via l'appel systeme execveat dans Sudo jusqu'a la version 1.9.17p2.	29/08/2026	CVE-2026-82474	<= 1.9.17p2	Mettre a jour sudo vers la derniere version disponible	7.8

II.3 CMS

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
WPLP Cookie Consent (WordPress)	Vulnerabilite critique dans le plugin WordPress WPLP Cookie Consent (banniere de cookies, GDPR/CCPA) permettant une comp	01/09/2026	CVE-2026-75865	Plugin WordPress	Mettre a jour le plugin WPLP Cookie Consent	9.8
ProfilePress (WordPress)	Execution de code arbitraire a distance sans authentification dans le plugin WordPress ProfilePress (wp-user-avatar) ava	31/08/2026	CVE-2026-66047	< 4.17.2	Mettre a jour ProfilePress vers la version 4.17.2 ou superieure	8.1
Support Genix (WordPress)	Vulnerabilite dans le plugin WordPress Support Genix (helpdesk, chatbot IA) permettant une compromission du site.	01/09/2026	CVE-2026-19806	Plugin WordPress	Mettre a jour le plugin Support Genix	8.8
Frontend Admin (WordPress)	Suppression arbitraire de fichiers dans le plugin WordPress Frontend Admin by DynamiApps due a une verification insuffis	01/09/2026	CVE-2026-19952	Plugin WordPress	Mettre a jour le plugin Frontend Admin	7.5

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
SeaCMS	Injection de commandes dans la fonction parseIf du fichier search.php de SeaCMS jusqu'a la version 13.6.	31/08/2026	CVE-2026-82598	<= 13.6	Mettre a jour SeaCMS vers la derniere version disponible	7.3

II.4 Autres

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
PaperCut NG / MF	Controle d'acces inapproprie dans l'interface d'administration web de PaperCut NG et MF. Vulnrabilite ajoutee au catalog	28/08/2026	CVE-2026-81578	NG / MF	Appliquer le correctif PaperCut des que possible	9.8
PaperCut NG / MF	Chargement dynamique de classe non securise dans les utilitaires de connexion base de donnees de PaperCut NG et MF. Ajou	28/08/2026	CVE-2026-82078	NG / MF	Appliquer le correctif PaperCut des que possible	9.1
Gitea	Execution de code a distance via l'API diffpatch par installation de hooks Git dans Gitea avant la version 1.27.1. Ajout	26/08/2026	CVE-2026-60004	< 1.27.1	Mettre a jour Gitea vers la version 1.27.1 ou superieure	9.8
TrueConf Server	Authentification manquante dans TrueConf Server permettant a un attaquant distant non authentifie d'executer du code via	19/08/2026	CVE-2026-72529	Versions concernees	Mettre a jour TrueConf Server vers la derniere version	9.8
argocd-mcp	argocd-mcp 0.8.0 lie son transport HTTP a toutes les interfaces reseau et accepte les sessions MCP sans authentification	29/08/2026	CVE-2026-82456	0.8.0	Mettre a jour argocd-mcp vers la derniere version	10.0
QVidium Opera11	Vulnerabilite critique dans le fichier /cgi-bin de QVidium Opera11 3.3.2a26-Ax4x-opera11 permettant une compromission to	31/08/2026	CVE-2026-82971	3.3.2a26-Ax4x-opera11	Contacter l'editeur pour obtenir un correctif	10.0
Oracle Reports Developer	Vulnerabilite dans le produit Oracle Reports Developer de Oracle Fusion Middleware (composant Security and Auth) permett	18/08/2026	CVE-2026-70670	Fusion Middleware	Appliquer le correctif du Critical Patch Update Oracle	9.6
Apache APISIX	Confiance en des entrees non fiables dans une decision de securite dans Apache APISIX permettant de contourner les contr	26/08/2026	CVE-2026-63041	Versions concernees	Mettre a jour Apache APISIX vers la derniere version	8.8

III. Actualites

UNITEL retablit ses services mobiles apres une cyberattaque en juillet

L'operateur de telecommunications angolais UNITEL a finalement restaure l'ensemble de ses services mobiles a travers le pays, plusieurs semaines apres une cyberattaque qui avait perturbe ses infrastructures. L'incident illustre la vulnerabilite croissante des operateurs de telecommunications africains face aux attaques informatiques.

Source: TechAfrica News - 21/08/2026

Les PME africaines face a la montee des cybermenaces

Selon ITWeb Africa, les petites et moyennes entreprises du continent sont de plus en plus ciblees par les cybercriminels, faute de ressources dediees a la cybersecurite. Les experts appellent a renforcer la sensibilisation et l'adoption de mesures de protection de base (MFA, sauvegardes, correctifs).

Source: ITWeb Africa - 01/09/2026

Le Nigeria se tourne vers le cloud souverain pour sa cybersecurite nationale

Le Nigeria envisage de deployer des infrastructures de cloud souverain afin de proteger ses donnees sensibles et de renforcer sa securite nationale face aux menaces cyber. Cette initiative s'inscrit dans une dynamique plus large de souverainete numerique sur le continent.

Source: Dark Reading - 26/08/2026

Le Mozambique renforce son cadre de cybersecurite face aux menaces numeriques

Le Mozambique a annonce un renforcement de son cadre juridique et technique de cybersecurite, l'agence nationale INTIC alertant sur la croissance des menaces numeriques dans le pays. Une dynamique similaire est observee dans plusieurs Etats d'Afrique centrale et de l'Ouest.

Source: Tech Review Africa - 29/08/2026

Investissement de 75 millions USD dans un centre de donnees IA au Cameroun

La societe Cybastion envisage d'investir environ 75 millions de dollars dans un centre de donnees dedie a l'intelligence artificielle et une centrale electrique au Cameroun. Ce projet, qui renforcerait les infrastructures numeriques nationales, devra s'accompagner de garanties solides en matiere de cybersecurite.

Source: Pan African Visions - 01/09/2026

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.