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 June 2026

Publication date: 15/06/2026

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
Google Chrome	Use after free dans FileSystem dans Google Chrome avant 149.0.7827.53 permettant a un attaquant distant de realiser une	04/06/2026	CVE-2026-10931	149.0.7827.53	Mettre a jour Google Chrome vers la version 149.0.7827.53 ou superieure	9.6
Google Chrome	Implementation inadequate dans Codecs dans Google Chrome avant 149.0.7827.53 permettant a un attaquant distant de realis	04/06/2026	CVE-2026-10966	149.0.7827.53	Mettre a jour Google Chrome vers la version 149.0.7827.53 ou superieure	9.6
Google Chrome (Windows)	Validation insuffisante des entrees dans Printing dans Google Chrome sur Windows avant 149.0.7827.53 permettant a un att	04/06/2026	CVE-2026-10971	149.0.7827.53	Mettre a jour Google Chrome vers la version 149.0.7827.53 ou superieure	9.6
Google Chrome (Linux)	Use after free dans Ozone dans Google Chrome sur Linux avant 149.0.7827.53 permettant a un attaquant distant de realiser	04/06/2026	CVE-2026-10972	149.0.7827.53	Mettre a jour Google Chrome vers la version 149.0.7827.53 ou superieure	9.6
Google Chrome (Android)	Validation insuffisante des entrees dans Drag and Drop dans Google Chrome sur Android avant 149.0.7827.53 permettant a u	04/06/2026	CVE-2026-11029	149.0.7827.53	Mettre a jour Google Chrome vers la version 149.0.7827.53 ou superieure	9.6

II.2 Operating Systems

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Android	Dans addInputMethodListener, absence de verification de permission pouvant entrainer une elevation de privilege locale s	01/06/2026	CVE-2026-0072	Android XR	Appliquer le correctif de securite Android de juin 2026	7.8
Android	Plusieurs emplacements contiennent une divulgation d'images entre utilisateurs due a une validation inadequate des entre	01/06/2026	CVE-2025-22424	Android	Appliquer le correctif de securite Android de juin 2026	7.8
Android	Plusieurs emplacements permettent un lancement d'activite en arriere-plan du a un controle de permission manquant, condu	01/06/2026	CVE-2025-32348	Android	Appliquer le correctif de securite Android de juin 2026	7.8
Linux Kernel	Le noyau Linux contient une vulnerabilite d'authentification inadequate dans cgroups v1 release_agent, permettant une el	02/06/2026	CVE-2022-0492	Noyau Linux (cgroups v1)	Appliquer les correctifs de securite du noyau Linux ou desactiver cgroups v1	7.8

II.3 CMS

Vulnerability	Description	Date	CVE	Version	Solution	CVSS

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
WordPress Kirki Plugin	Le plugin Kirki pour WordPress est vulnerable a une elevation de privilege via prise de controle de compte dans toutes l	02/06/2026	CVE-2026-8206	Toutes versions	Mettre a jour le plugin Kirki vers la version la plus recente	9.8
WordPress ARMember Plugin	Le plugin ARMember Premium pour WordPress est vulnerable a un mecanisme de reinitialisation de mot de passe non securise	02/06/2026	CVE-2026-5076	7.3.1 et inferieures	Mettre a jour le plugin ARMember Premium vers la version 7.3.2 ou superieure	9.8
WordPress Hippoo WooCommerce Plugin	Le plugin Hippoo Mobile App pour WooCommerce est vulnerable a un contournement d'authentification menant a la prise de c	05/06/2026	CVE-2026-10580	Toutes versions	Mettre a jour le plugin Hippoo Mobile App vers la version la plus recente	9.8
WordPress Seotheme	WordPress Seotheme contient une vulnerabilite d'execution de code a distance permettant a des attaquants non authentifie	08/06/2026	CVE-2023-54352	Toutes versions	Mettre a jour le theme Seotheme ou le supprimer	9.8
WordPress Background Image Cropper	WordPress Background Image Cropper version 1.2 contient une vulnerabilite d'execution de code a distance permettant a de	08/06/2026	CVE-2024-58348	1.2	Desactiver ou supprimer le plugin Background Image Cropper	9.8

II.4 Others

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Microsoft Azure HorizonDB	Contournement d'authentification par usurpation dans Azure HorizonDB permettant a un attaquant non autorise d'elever ses	04/06/2026	CVE-2026-48567	Azure HorizonDB	Appliquer les correctifs Microsoft conformement aux	10.0
IBM WebSphere Application Server	IBM WebSphere Application Server 9.0 et 8.5 est vulnerable a une usurpation d'identite permettant a un attaquant de se f	01/06/2026	CVE-2026-8644	9.0, 8.5	Appliquer le correctif IBM pour WebSphere Application Server	9.1
IBM WebSphere Application Server	IBM WebSphere Application Server 9.0 et 8.5 est vulnerable a une execution de code a distance causee par le contournemen	01/06/2026	CVE-2026-9311	9.0, 8.5	Appliquer le correctif IBM pour WebSphere Application Server	9.0
IBM WebSphere Application Server	IBM WebSphere Application Server 9.0 et 8.5 est vulnerable a une execution de code a distance potentielle due a la deser	01/06/2026	CVE-2026-9319	9.0, 8.5	Appliquer le correctif IBM pour WebSphere Application Server	9.0
IBM i Access Family	IBM i Access Family 1.1.5.0 a 1.1.9.12 - IBM i Access Client Solutions (ACS) est vulnerable a une execution de code a di	01/06/2026	CVE-2026-7770	1.1.5.0 - 1.1.9.12	Mettre a jour IBM i Access Family vers la version 1.1.9.13 ou superieure	8.8
Apache Solr	Identifiants hardcodes dans l'outil de configuration Basic Authentication d'Apache Solr versions 9.4.0 a 9.10.1 et 10.0.	01/06/2026	CVE-2026-44825	9.4.0 - 9.10.1, 10.0.0	Mettre a jour Apache Solr vers une version corrigee	8.1

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Microsoft SharePoint	Deserialisation de donnees non fiables dans Microsoft Office SharePoint permettant a un attaquant autorise d'executer du	01/06/2026	CVE-2026-47294	SharePoint Server	Appliquer le correctif de securite Microsoft de juin 2026	8.0
Check Point Security Gateway	Vulnerabilite d'authentification inadequate dans IKEv1 sur Check Point Security Gateway permettant a un attaquant distan	08/06/2026	CVE-2026-50751	Security Gateway (IKEv1)	Appliquer les correctifs Check Point conformement aux instructions du fabricant	8.6
Oracle PeopleSoft Enterprise PeopleTools	Vulnerabilite d'authentification manquante dans Oracle PeopleSoft Enterprise PeopleTools permettant a un attaquant non a	12/06/2026	CVE-2026-35273	PeopleTools	Appliquer les correctifs Oracle conformement aux instructions du fabricant	9.1
Ivanti Sentry	Vulnerabilite d'injection de commandes OS dans Ivanti Sentry (anciennement MobileIron Sentry) permettant a un utilisateu	11/06/2026	CVE-2026-10520	Ivanti Sentry	Appliquer les correctifs Ivanti conformement aux instructions du fabricant	9.8
Oracle WebLogic Server	Vulnerabilite non specifiee dans Oracle WebLogic Server permettant a un attaquant non authentifie avec acces reseau via	01/06/2026	CVE-2024-21182	WebLogic Server	Appliquer les correctifs Oracle conformement aux instructions du fabricant	9.8

III. News

Cameroon Strengthens Cybersecurity with Advanced Systems at National CIRT

Le Cameroun renforce sa cybersecurite avec des systemes avances deployes au CIRT national, selon TechAfrica News. Le pays continue d'investir dans la protection de son economie numerique face a la hausse des cyberattaques.

Source: TechAfrica News - techafricanews.com

Cameroon Invests FCFA 735 million to Shield Digital Economy from Cyber Threats

Le Cameroun investit 735 millions de FCFA pour proteger son economie numerique contre les cybermenaces. Le financement vise a renforcer les infrastructures de securite informatique nationales.

Source: Business in Cameroon - businessincameroon.com

ST Digital, Rhopen Labs Launch Africa's First Cybersecurity Operations Center

ST Digital et Rhopen Labs lancent le premier centre d'operations de cybersecurite en Afrique, marquant une etape importante dans la capacite du continent a repondre aux incidents de securite informatique.

Source: Business in Cameroon - businessincameroon.com

CYSEC AFRICA 2026 to Convene Africa's Cybersecurity Leaders in Johannesburg

CYSEC AFRICA 2026 reunira les leaders africains de la cybersecurite a Johannesburg pour discuter des defis et opportunites du continent en matiere de securite numerique.

Source: Asia Pacific Security Magazine

ICCA Launched in Rwanda to Strengthen Africa's Cybersecurity Collaboration

L'ICCA (International Cybersecurity Collaboration Alliance) a ete lancee au Rwanda pour renforcer la collaboration en matiere de cybersecurite en Afrique, reunissant des experts de tout le continent.

Source: TechAfrica News - techafricanews.com

Cybersecurity Tops Risk List for African Businesses in 2026

La cybersecurite est le principal risque identifie par les entreprises africaines en 2026, selon un nouveau rapport. Les organisations du continent font face a une augmentation significative des menaces numeriques.

Source: TechAfrica News - techafricanews.com

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.