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°1 of June 2026

Publication date: 08/06/2026

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 in PDFium component allowing remote code execution via crafted PDF file	28/05/2026	CVE-2026-10002	Chrome < 148.0.7778.216	Mettre a jour Chrome vers 148.0.7778.216	8.8
Google Chrome	Use-after-free dans SVG permettant execution de code arbitraire via page HTML malveillante	28/05/2026	CVE-2026-10007	Chrome < 148.0.7778.216	Mettre a jour Chrome vers 148.0.7778.216 ou superieur	8.8
Google Chrome	Use-after-free dans WebCodecs permettant execution de code arbitraire via page HTML	28/05/2026	CVE-2026-10013	Chrome < 148.0.7778.216	Mettre a jour Chrome vers 148.0.7778.216	8.8
Google Chrome	Use-after-free dans Passwords sur Windows permettant escalade de privileges apres compromission du renderer	28/05/2026	CVE-2026-10000	Chrome Windows < 148.0.7778.216	Mettre a jour Chrome vers 148.0.7778.216 ou superieur	8.3
Firefox	Condition limite incorrecte dans le composant Graphics: Text permettante execution de code arbitraire	02/06/2026	CVE-2026-10701	Firefox < 151.0.3	Mettre a jour Firefox vers 151.0.3 ou superieur	7.5

II.2 Operating Systems

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Android Framework	Debordement d'entier dans le Framework Android permettant elevation de privileges localement sans interaction utilisateu	01/06/2026	CVE-2025-48595	Android 14-16 (correctifs juin 2026)	Installer le correctif de securite Android	8.4
macOS (Apple)	Probleme de logique dans macOS Sequoia 15.7, Sonoma 14.8, Tahoe 26 permettant a une app malveillante d'elever ses privil	26/05/2026	CVE-2025-43306	macOS < Sequoia 15.7, Sonoma 14.8, Tahoe 26	Mettre a jour macOS vers Sequoia 15.7 / Sonoma 14.8 / Tahoe 26	7.8
macOS (Apple)	Condition de course dans macOS permettant a une application d'obtenir les	26/05/2026	CVE-2025-46284	macOS < Sequoia 15.7,	Mettre a jour macOS vers Sequoia 15.7 /	7.0
OpenVPN Connect (macOS)	Escalade de privileges via le service background d'OpenVPN Connect sur macOS permettant execution de commandes arbitrair	26/05/2026	CVE-2026-9560	OpenVPN Connect 3.5.1 a 3.8.1 sur macOS	Mettre a jour OpenVPN Connect vers une version corrigee	7.8
Canonical Multipass (macOS)	Correction incomplete de CVE-2025-5199 dans Multipass pour macOS avant 1.16.3, contournement du correctif de securite	28/05/2026	CVE-2026-49237	Multipass macOS < 1.16.3	Mettre a jour Multipass vers version 1.16.3 ou superieure	7.8

II.3 CMS

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Mirasvit Full Page Cache Warmer (Magento 2)	Injection d'objet PHP (deserialisation) permettant a un attaquant non authentifie d'executer du code a distance	26/05/2026	CVE-2026-45247	Mirasvit Full Page Cache Warmer <	Mettre a jour le plugin Mirasvit Full Page Cache Warmer vers	9.8
Joomla JE Photo Gallery	Injection SQL dans le composant Joomla JE Photo Gallery 1.1 permettant a un attaquant non authentifie d'executer des com	01/06/2026	CVE-2018-25433	Joomla Component JE Photo Gallery 1.1	Mettre a jour le composant JE Photo Gallery ou le desactiver	8.2
Drupal SAML SSO - Service Provider	Gestion incorrecte des conditions exceptionnelles permettant une elevation de privileges dans le module SAML SSO	28/05/2026	CVE-2026-5343	Drupal SAML SSO Service Provider (versions concernees)	Appliquer le correctif Drupal pour le module SAML SSO	7.4

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
EventPress WordPress Theme	Absence d'echappement et de validation du parametre 'id' dans l'action AJAX eventpress_customizer_notify_dismiss_action	27/05/2026	CVE-2026-6268	EventPress theme WordPress < 22.2	Mettre a jour le theme EventPress vers version 22.2 ou superieure	7.1

II.4 Others

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Check Point Security Gateway	Defaut de validation de certificats IKEv1 contournant l'authentification VPN sans mot de passe. Activement exploite par	08/06/2026	CVE-2026-50751	Check Point R82.10 avant JHF Take 20	Appliquer le Jumbo Hotfix. Desactiver IKEv1 si possible	9.3
Check Point Security Gateway (AitM)	Attaque adversary-in-the-middle sur IKEv1 permettant de contourner la validation de certificats dans les connexions VPN	08/06/2026	CVE-2026-50752	Check Point (meme version que CVE-2026-50751)	Appliquer le meme correctif que	7.4
SolarWinds Serv-U	Consommation de ressources non controlee via requetes POST avec Content-Encoding: deflate, plantant le service sans auth	04/06/2026	CVE-2026-28318	SolarWinds Serv-U 15.5.4 HF1	Mettre a jour Serv-U. Appliquer les etapes d'attenuation	7.5
Cisco Catalyst SD-WAN Manager	Vulnerabilite dans le CLI de Cisco Catalyst SD-WAN Manager (anciennement SD-WAN vManage) permettant a un attaquant local	04/06/2026	CVE-2026-20245	Cisco Catalyst SD-WAN Manager (versions concernees)	Appliquer les correctifs Cisco	7.8
Nx Console (Supply Chain)	Version malveillante 18.95.0 de Nx Console publiee le 19 mai 2026 contenant du code malveillant. Retiree rapidement mais	27/05/2026	CVE-2026-48027	Nx Console 18.95.0	Eviter ou supprimer la version 18.95.0. Mettre a jour vers la derniere version stable	9.8

III. News

Cyberattacks a growing threat to South Africa's healthcare system

South Africa's healthcare sector is facing an increasing wave of cyberattacks, with hospitals and medical facilities becoming prime targets for ransomware and data breaches. The article highlights how the digitisation of health records and medical systems has expanded the attack surface, putting patient data and critical healthcare operations at risk.

Source: TimesLIVE

Wave of supercharged cyberattacks will hit South Africa within 5 months, expert warns

Cybersecurity experts have warned that South Africa faces a surge of sophisticated, AI-powered cyberattacks within the next five months. The warning comes as threat actors increasingly leverage generative AI tools to craft more convincing phishing campaigns and automate attack vectors targeting South African organizations across all sectors.

Source: MyBroadband

Don't let cyber attacks become your organisation's only legacy

The Namibia Economist warns that organisations across Namibia and Africa must prioritise cybersecurity as cyber threats continue to escalate. The piece emphasises that without proactive investment in security measures and employee awareness training, businesses risk catastrophic data breaches that could become their defining legacy.

Source: Namibia Economist

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.