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 July 2026

Publication date: 01/07/2026

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
Adobe Acrobat PDF Extension (Chrome)	Extension Chrome Adobe Acrobat PDF versions 26.5.2.2 et anterieures, une vulnerabilite UXSS de divulgation de donnees in	17/06/2026	CVE-2026-48294	26.5.2.2	Mettre a jour l'extension vers la version 26.5.2.3 ou ulterieure	7.4
Chromium V8 (Google Chrome/Edge)	Vulnerabilite de lecture/ecriture hors limites dans le moteur JavaScript V8 de Chromium, deja exploitee dans la nature (	17/06/2026	CVE-2026-11645	Toutes versions anterieures a 148.0.3967.83	Mettre a jour Chrome/Edge vers la derniere version stable	8.8

II.2 Operating Systems

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Android (Plusieurs composants AOSP)	De multiples vulnerabilites dans Android (elevation de privileges NFC, contournement de restrictions operateur, contourn	17/06/2026	CVE-2026-0063 / CVE-2026-0068 / CVE-2026-0071 / CVE-2026-0081 / CVE-2026-0082 / CVE-2026-0083	Android (plusieurs versions)	Appliquer le patch de securite Android de juin 2026	7.8
libssh2 (Multi-plateforme)	Vulnerabilite d'ecriture hors limites dans ssh2_transport_read() de libssh2 (versions jusqu'a 1.11.1). Un attaquant dist	17/06/2026	CVE-2026-55200	libssh2 <= 1.11.1	Mettre a jour libssh2 vers la version corrigee (commit 7acf3df)	8.1

II.3 CMS

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
SP Page Builder (Joomla)	Vulnerabilite critique dans l'extension SP Page Builder pour Joomla permettant a un attaquant non authentifie de telever	20/06/2026	CVE-2026-48908	Toutes versions concernees	Mettre a jour l'extension SP Page Builder vers la derniere version disponible	9.8
iCagenda (Joomla)	Vulnerabilite dans l'extension iCagenda pour Joomla permettant le televersement de fichiers arbitraires via la fonctionn	20/06/2026	CVE-2026-48939	Toutes versions concernees	Mettre a jour l'extension iCagenda vers la derniere version disponible	9.8
Contest Gallery (WordPress)	Plugin WordPress Contest Gallery versions inferieures ou egales a 30.0.2, vulnerabilite d'elevation de privileges via le	17/06/2026	CVE-2026-12165	<= 30.0.2	Mettre a jour le plugin Contest Gallery vers la version 30.0.3 ou ulterieure	8.8

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
JetEngine (WordPress)	Plugin WordPress JetEngine versions jusqu'a 3.8.10.1, vulnerabilite d'injection SQL dans le handler AJAX listing_load_mo	17/06/2026	CVE-2026-12360	<= 3.8.10.1	Mettre a jour le plugin JetEngine vers la version 3.8.11 ou ulterieure	7.5
Cacti	Framework de gestion de performances Cacti versions 1.2.30 et anterieures. Vulnerabilite d'injection de commande via la	25/06/2026	CVE-2026-40079	<= 1.2.30	Mettre a jour Cacti vers la version 1.2.31 ou ulterieure	9.8

II.4 Others

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
Apache DolphinScheduler	Absence de verification d'autorisation sur l'API DataSource permettant la divulgation non autorisee des metadonnees des	17/06/2026	CVE-2026-32966	< 3.4.2	Mettre a jour Apache DolphinScheduler vers la version 3.4.2 ou ulterieure	9.8
PTC Windchill / FlexPLM (CISA KEV)	Vulnerabilite critique d'exection de code a distance (RCE) via deserialisation de donnees non fiables dans PTC Windchill	18/06/2026	CVE-2026-12569	Toutes versions concernees	Appliquer le correctif PTC recommande (consulter le bulletin PTC)	9.8
JetBrains Hub	Contournement d'authentification par acces direct a la base de donnees dans JetBrains Hub permettant a un attaquant d'ob	19/06/2026	CVE-2026-50242	Avant 2026.1.13757	Mettre a jour JetBrains Hub vers la version 2026.1.13757 ou ulterieure	10.0
Traefik (Reverse Proxy)	De multiples vulnerabilites critiques dans Traefik (versions avant 2.11.48, 3.6.19 et 3.7.3) : contournement du middlewa	23/06/2026	CVE-2026-48020 / CVE-2026-48491 / CVE-2026-53622	< 2.11.48, < 3.6.19, < 3.7.3	Mettre a jour Traefik vers la version 3.7.3 ou ulterieure	10.0
n8n (Workflow Automation)	Multiples vulnerabilites critiques dans n8n (versions avant 2.25.7 et 2.26.2) : contournement d'authentification sur l'e	23/06/2026	CVE-2026-54309 / CVE-2026-54310 / CVE-2026-44789	< 2.25.7, < 2.26.2	Mettre a jour n8n vers la version 2.25.7 ou 2.26.2	10.0
Apache APISIX (Multiples plugins)	Plusieurs vulnerabilites dans Apache APISIX : contournement d'authentification via jwt-auth (CVE-2026-39999, CVSS 9.1),	19/06/2026	CVE-2026-39999 / CVE-2026-44087 / CVE-2026-49230 / CVE-2026-49871	Toutes versions concernees	Mettre a jour Apache APISIX et desactiver les plugins vulnerables si non utilises	9.3
Feast (Feature Store)	Vulnerabilite de deserialisation non securisee dans Feast avant la version 0.63.0, permettant a un attaquant non authent	24/06/2026	CVE-2026-56121	< 0.63.0	Mettre a jour Feast vers la version 0.63.0 ou ulterieure	9.8

Vulnerability	Description	Date	CVE	Version	Solution	CVSS
M365 Copilot	Absence d'authentification pour une fonction critique dans M365 Copilot permettant a un attaquant non autorise de divulg	18/06/2026	CVE-2026-54130	Toutes versions concernees	Appliquer les correctifs Microsoft de juin 2026	9.8
LiteLLM (AI Gateway)	Execution de code a distance (RCE) dans LiteLLM avant la version 1.84.0. L'API Gateway AI permet a un attaquant non auth	22/06/2026	CVE-2026-49468	< 1.84.0	Mettre a jour LiteLLM vers la version 1.84.0 ou ulterieure	9.8

III. News

Mastercard lance un Centre d'Excellence de Cybersecurite en Afrique

Mastercard a inaugure l'Africa Cybersecurity Center of Excellence en Afrique du Sud pour renforcer la securite numerique du continent. Le centre vise a former les professionnels locaux, developper des solutions adaptees aux menaces africaines, et soutenir les gouvernements dans l'elaboration de cadres reglementaires. Cette initiative repond a l'augmentation de 45% des cyberattaques ciblant les institutions financieres africaines en 2026.

Source: Mastercard / TechAfrica News - 29 Juin 2026

Le Kenya met en place une Agence Nationale de Cybersecurite

Le Kenya a officialise la creation de sa National Cybersecurity Agency pour renforcer les defenses numeriques du pays. L'agence sera chargee de la coordination des reponses aux incidents, de la sensibilisation du public et de la collaboration avec les partenaires internationaux. Cette decision fait suite a une hausse significative des cyberattaques ciblant les infrastructures critiques kenyanes.

Source: CIO Africa - 23 Juin 2026

Ethiopie renforce ses defenses cybersecurite avec l'acceleration de la transformation numerique

L'Ethiopie a annonce un renforcement de ses capacites de cybersecurite alors que le pays accelere sa transformation numerique. Ethio telecom a renforce son leadership en matiere de cybersecurite lors de l'ICCA2026, un evenement panafricain dedie a la collaboration en cybersecurite. Le pays investit dans la formation de specialistes et la mise en place de centres de operations de securite (SOC).

Source: Dawan Africa / TechAfrica News - 25 Juin 2026

Africa Internet Summit 2026 : la cybersecurite et les infrastructures au coeur des debats a Nairobi

L'Africa Internet Summit 2026 s'est tenu a Nairobi, reunissant les parties prenantes du numerique africain pour aborder les defis de cybersecurite et d'infrastructures. Les discussions ont porte sur la securisation des routes Internet, la gouvernance de l'Internet et la resilience face aux cyberattaques transfrontalieres.

Source: Stream Africa - 23 Juin 2026

Nigeria remporte le grand prix du Hackathon Regional de Cybersecurite de la CEDEAO 2026

Le Nigeria a remporte le grand prix de 10 000 dollars lors de la 4eme edition du Hackathon Regional de Cybersecurite de la CEDEAO qui s'est tenue a Accra, Ghana. L'evenement vise a stimuler l'innovation en matiere de cybersecurite dans la region ouest-africaine et a renforcer les competences des jeunes talents numeriques.

Source: TechAfrica News - 14 Juin 2026

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.