

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 Octobre 2026

Date de publication: 15/10/2026

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	6
IV. Notes importantes	7

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
Google Chrome	Fuite d'informations dans le module Permissions permettant a un attaquant distant de contourner l'isolation des sites vi	06/10/2026	CVE-2026-106237	avant 155.0.8059.39	Mettre a jour Chrome vers la version 155.0.8059.39 ou	9.6
Google Chrome (macOS)	Autorisation incorrecte dans Chromoting permettant de contourner les restrictions d'accès système et de prendre le contr	06/10/2026	CVE-2026-106195	avant 155.0.8059.39	Mettre a jour Chrome vers la version 155.0.8059.39 ou	9.1
Google Chrome (Android)	Confused deputy dans les WebAPKs : un attaquant distant peut contourner la politique d'origine web par ingenierie social	06/10/2026	CVE-2026-106221	avant 155.0.8059.39	superieure Mettre a jour Chrome sur Android vers la version	8.3
Google Chrome	Absence d'autorisation dans le composant FileSystem : un attaquant ayant compromis le processus de rendu peut contourner	06/10/2026	CVE-2026-106198	avant 155.0.8059.39	Mettre a jour Chrome vers la version 155.0.8059.39 ou	8.2
Google Chrome (iOS)	Absence d'autorisation dans la navigation permettant d'atteindre une page privilegiee et de contourner la politique d'or	06/10/2026	CVE-2026-106196	avant 155.0.8059.39	superieure Mettre a jour Chrome sur iOS vers la version 155.0.8059.39	7.6

II.2 Systemes d'exploitation

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Microsoft Windows	Vulnérabilité d'authentification manquante pour une fonction critique dans Windows Credential Guard, permettant a un att	13/10/2026	CVE-2026-70580	Windows (Credential Guard)	Appliquer le correctif Microsoft du mois d'octobre 2026	8.8
Juniper Junos OS	Authentification incorrecte dans l'interface d'administration J-Web et NETCONF : un attaquant non authentifie peut obten	14/10/2026	CVE-2026-101954	Junos OS et Junos OS Evolved	Appliquer les correctifs Juniper de l'avis JSA du 14 octobre 2026	9.8
Lantronix XPress-DR	Authentification manquante sur le protocole de configuration UDP (port 30718) permettant de lire et de reecrire de facon	14/10/2026	CVE-2026-109439	firmware jusqu'a 8.1.0.0	Restreindre l'accès réseau au port 30718 ou remplacer le	9.8
Xen Orchestra	Controle d'accès inadapte permettant a tout utilisateur authentifie de devenir administrateur global en abusant des meth	13/10/2026	CVE-2026-110111	avant 6.9.0	Mettre a jour Xen Orchestra vers la version 6.9.0 ou superieure	7.5

II.3 CMS

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
WordPress - AGE-GATE	Execution de code a distance via le parametre width/height, l'endpoint admin.php ne chargeant pas WordPress et n'effectu	14/10/2026	CVE-2026-104800	AGE-GATE jusqu'a 1.0	Desactiver l'extension AGE-GATE en attendant un	9.8
WordPress - 10Web Booster	Televersement arbitraire de fichiers via la fonction compressCustom permettant l'execution de code a distance sans auth	15/10/2026	CVE-2026-108587	10Web Booster jusqu'a 2.34.10	Mettre a jour 10Web Booster ou le desactiver	9.8

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
WordPress - Snazzy Social Media Feed	Televersement arbitraire de fichiers via le script save-to-cache.php depourvu des controles d'authentification et de non	14/10/2026	CVE-2026-110002	Snazzy Social Media Feed jusqu'a 2.5	Mettre a jour ou desactiver l'extension	9.8
WordPress - Abandoned Cart Pro (WooCommerce)	Injection SQL via le champ meta_value du panier invite, exploitable par un attaquant pour extraire des donnees de la bas	14/10/2026	CVE-2026-97668	Abandoned Cart Pro jusqu'a 10.8.0	Mettre a jour Abandoned Cart Pro au-dela de la version 10.8.0	9.8
WordPress - SimpleForm	Elevation de privileges via l'action AJAX non authentifiee simpleform_wp_register permettant l'attribution de roles arbi	14/10/2026	CVE-2026-104748	SimpleForm jusqu'a 3.10.0	Mettre a jour ou desactiver l'extension	9.8
Joomla - OrdaSoft CCK	Injection SQL non authentifiee dans le tri des enregistrements, la colonne order etant fournie par l'utilisateur sans va	05/10/2026	CVE-2026-102428	OrdaSoft Joomla CCK avant 8.3.16	Mettre a jour OrdaSoft CCK vers la version 8.3.16 ou superieure	9.8
Joomla - TF Content	Publication non authentifiee de contenus et affectation massive de proprietes (published, access, created_by) via le con	05/10/2026	CVE-2026-102780	TF Content 2.9.0 - 2.9.4	Mettre a jour TF Content vers une version corrgee	9.8
WordPress - Click to Chat WhatsApp	Execution arbitraire de shortcodes via la fonction greetings_dialog() exploitant le parametre REQUEST_URI non filtre.	14/10/2026	CVE-2026-92097	Click to Chat jusqu'a 4.44	Mettre a jour Click to Chat au-dela de la version 4.44	9.1

II.4 Autres

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Juniper Junos OS - rpd (BGP)	Debordement de tampon dans le demon de routage rpd : un pair BGP peut provoquer un crash ou l'execution de code a distan	14/10/2026	CVE-2026-101990	Junos OS et Junos OS Evolved	Appliquer les correctifs Juniper de l'avis JSA du 14 octobre 2026	9.8
Juniper Junos OS - SRX	Debordement de tampon dans le composant SVR des series SRX : un attaquant reseau non authentifie peut provoquer un deni	14/10/2026	CVE-2026-101950	Junos OS sur series SRX	Appliquer les correctifs Juniper de l'avis JSA du 14 octobre 2026	9.8
Cisco NX-OS	Multiples debordements d'ecriture hors limites (CWE-787) corriges dans une version de durcissement logiciel du systeme d	07/10/2026	CVE-2026-76459	Cisco NX-OS	Appliquer la mise a jour de durcissement Cisco NX-OS	9.8
Brocade Fabric OS	Contournement d'autorisation critique dans le serveur de gestion : un commutateur compromis peut executer des actions d'	08/10/2026	CVE-2026-87659	Brocade Fabric OS avant 10.0.1	Mettre a jour Brocade Fabric OS vers la version 10.0.1	9.8
Brocade Fabric OS - SNMP	Debordement de tampon dans le demon SNMP : un attaquant distant non authentifie peut provoquer une corruption memoire ou	08/10/2026	CVE-2026-87684	Brocade Fabric OS avant 10.0.1	Mettre a jour Brocade Fabric OS vers la version 10.0.1	9.8
Cisco License On-Prem	Validation d'entree inadapte et absence d'authentification dans l'API de gestion, permettant a un attaquant non authenti	07/10/2026	CVE-2026-76454	Cisco Smart Licensing Utility API	Appliquer le correctif Cisco pour Cisco License On-Prem	9.1
Apache Jackrabbit	Fixation et reutilisation de session entre utilisateurs : le serveur WebDAV rattache une session authentifiee mise en ca	07/10/2026	CVE-2026-92414	Jackrabbit 2.23.0-2.23.5, 2.22.0-2.22.4, 2.20.0-2.20.17	Mettre a jour vers 2.23.6, 2.22.5 ou 2.20.18	9.1
PHPNuxBill	Injection SQL non authentifiee dans l'endpoint REST FreeRADIUS de radius.php permettant d'extraire des enregistrements c	09/10/2026	CVE-2026-108107	PHPNuxBill jusqu'a 2025.3.20	Appliquer le correctif PHPNuxBill ou restreindre l'accès a l'endpoint	9.8

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Splunk Enterprise	Multiples vulnerabilites internes regroupees par type de faiblesse (CWE) corrigees dans la version de maintenance de Spl	07/10/2026	CVE-2026-76285	avant 10.4.3, 10.2.7, 10.0.10, 9.4.15	Mettre a jour Splunk Enterprise vers 10.4.3, 10.2.7, 10.0.10 ou 9.4.15	9.8
Dell Container Storage Modules	Utilisation d'identifiants codes en dur dans csm-docs : un attaquant distant non authentifie peut divulguer des informat	06/10/2026	CVE-2026-54472	avant 1.18.0	Mettre a jour Dell CSM vers la version 1.18.0 ou superieure	9.8

III. Actualites

Les cyberattaques contre les entreprises africaines augmentent plus vite que la moyenne mondiale

Selon des donnees publiees le 12 octobre 2026, les entreprises africaines subissent une hausse des cyberattaques superieure a la moyenne mondiale. Les secteurs de la finance, du commerce de detail et des telecommunications restent les plus vises, ce qui confirme la necessite pour les organisations camerounaises de renforcer leurs defenses et leur surveillance.

Source: Africa Business Communities

Le Kenya figure parmi les pays les plus attaques de la zone EMEA avec une hausse de 48%

Une analyse publiee le 12 octobre 2026 classe le Kenya parmi les pays les plus attaques de la region EMEA, avec une progression des incidents de 48%. Cette tendance regionale rappelle que l'Afrique de l'Est comme l'Afrique centrale font face a une pression croissante des groupes cybercriminels.

Source: Africa Business Communities

L'intelligence artificielle modifie la nature de la cybercriminalite en Afrique

Plusieurs analyses publiees debut octobre 2026 soulignent que l'intelligence artificielle abaisse le cout et la complexite des attaques, exposant davantage les petites entreprises et les commercants africains. Les experts appellent a une sensibilisation accrue et a l'adoption d'outils de detection adaptes a ces nouvelles menaces.

Source: ITWeb Africa / South African Government News Agency

La formation des equipes, priorite des partenariats cybersecurite en Afrique

Le 13 octobre 2026, un partenariat regional a ete annonce pour etendre les programmes de sensibilisation et de formation en cybersecurite a travers l'Afrique. La formation des collaborateurs reste l'un des leviers les plus efficaces pour reduire le risque d'hameconnage et d'erreur humaine.

Source: TechAfrica News

IV. Notes importantes

1. Veuillez enregistrer les adresses alerts@cirt.cm et alerts@cirt.antic.cm parmi vos contacts ou l'enregistrer comme expéditeur approuvé afin de ne plus recevoir les mails en provenance de cette adresse dans vos spam.
2. Ce document est produit régulièrement et téléchargeable sur notre site web www.cirt.cm. Vous y trouverez aussi des alertes et autres publications relatives à la cybersécurité et à la cybercriminalité.
3. CentOS 7 n'est plus supporté depuis juin 2024. L'utilisation des solutions ne possédant aucun support technique présente un risque élevé étant donné qu'aucun correctif ne sera émis après d'éventuelles vulnérabilités détectées.
4. Microsoft a mis fin au support de Windows 7 depuis le 14 janvier 2020. Il est recommandé de planifier la migration des postes utilisateurs utilisant encore ce système.