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 Novembre 2026

Date de publication: 15/11/2026

Classification: Publique

Sommaire

I. Lexique du Bulletin 3

II. Vulnerabilites publiees 4

II.1 Navigateurs 4

II.2 Systemes d'exploitation 4

II.3 CMS 5

II.4 Autres 5

III. Actualites 7

IV. Notes importantes 8

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	Use after free dans Prerender permettant a un attaquant distant d'executer du code arbitraire hors du bac a sable via un	03/11/2026	CVE-2026-121035	157.0.8103.38	Mettre a jour Google Chrome	9.6
Google Chrome	Depassement de tampon dans ANGLE (Windows) permettant l'execution de code arbitraire hors du bac a sable. Deja exploitee	10/11/2026	CVE-2026-125350	157.0.8103.50	Mettre a jour Google Chrome	8.8
Google Chrome	Autorisation incorrecte dans FileSystem exploitable par ingenierie sociale pour executer du code hors du bac a sable.	03/11/2026	CVE-2026-121060	157.0.8103.38	Mettre a jour Google Chrome	9.6
Google Chrome	Corruption memoire dans GPU (Android) permettant l'execution de code arbitraire hors du bac a sable.	03/11/2026	CVE-2026-121074	157.0.8103.38	Mettre a jour Google Chrome	9.6
Google Chrome	Autorisation incorrecte dans DevTools permettant, par ingenierie sociale, l'execution de code arbitraire hors du bac a	03/11/2026	CVE-2026-121030	157.0.8103.38	Mettre a jour Google Chrome	9.6
Google Chrome	Confusion de types dans le moteur V8 permettant l'execution de code arbitraire dans le bac a sable via une page HTML pie	03/11/2026	CVE-2026-121057	157.0.8103.38	Mettre a jour Google Chrome	8.8
Google Chrome	Lecture hors limites dans Skia permettant a un attaquant distant de lire la memoire hors du bac a sable.	03/11/2026	CVE-2026-121032	157.0.8103.38	Mettre a jour Google Chrome	7.4
Google Chrome	Course critique dans le moteur V8 permettant l'execution de code arbitraire dans le bac a sable. Google recommande la mi	03/11/2026	CVE-2026-121048	157.0.8103.38	Mettre a jour Google Chrome	8.8

II.2 Systemes d'exploitation

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Microsoft Windows	Elevation de privileges locale dans Windows Installer exploitant une condition de concurrence de type TOCTOU.	10/11/2026	CVE-2026-119398	Correctif cumulatif de novembre 2026	Appliquer les mises a jour Windows	7.8
Microsoft Windows	Depassement de tampon base sur le tas dans Windows Print Spooler permettant l'execution de code via le reseau.	10/11/2026	CVE-2026-119950	Correctif cumulatif de novembre 2026	Appliquer les mises a jour Windows	8.8
Microsoft Windows	Double liberation dans Remote Desktop Client permettant a un attaquant non authentifie d'executer du code via le reseau.	10/11/2026	CVE-2026-119934	Correctif cumulatif de novembre 2026	Appliquer les mises a jour Windows	8.8
Microsoft Windows	Depassement de tampon dans le controleur Storage Spaces permettant l'execution de code a distance sans authentification.	10/11/2026	CVE-2026-119908	Correctif cumulatif de novembre 2026	Appliquer les mises a jour Windows	8.8
Microsoft Windows	Depassement de tampon dans Active Directory permettant l'execution de code via le reseau par un attaquant authentifie.	10/11/2026	CVE-2026-119948	Correctif cumulatif de novembre 2026	Appliquer les mises a jour Windows	7.5
Microsoft Windows	Contournement de la politique d'authentification NTLM dans Windows Schannel exploitable sans authentification.	10/11/2026	CVE-2026-119952	Correctif cumulatif de novembre 2026	Appliquer les mises a jour Windows	8.1

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Synology DSM	Injection SQL dans l'API d'authentification de DSM permettant a un attaquant distant de lire et modifier des fichiers ar	12/11/2026	CVE-2026-76954	7.2.1-69057-13 / 7.3.2-86009-5 / 7.4.1-90080-1	Mettre a jour DiskStation Manager	9.8
Synology DSM	Contournement d'authentification par canal alternatif dans le service rsync de DSM permettant l'acces non autorise au NA	12/11/2026	CVE-2026-85101	7.2.1-69057-13 / 7.3.2-86009-5 / 7.4.1-90080-1	Mettre a jour DiskStation Manager	8.6
Linux (OpenSSH)	Contournement de l'authentification par mot de passe dans sshd lorsque OpenSSH est compile avec musl libc sans PAM.	05/11/2026	CVE-2026-123158	10.6p2	Mettre a jour OpenSSH	8.1
Linux (BusyBox)	Faille dans le client TFTP de BusyBox permettant la corruption de la memoire heap lors du traitement de reponses serveur	11/11/2026	CVE-2026-124737	Dernieres versions BusyBox	Mettre a jour le paquet BusyBox	7.5

II.3 CMS

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
WordPress (greffon Shipo)	Contournement d'authentification dans le greffon Shipo 1.6 a 1.8.0 permettant a un attaquant non authentifie de prendre	14/11/2026	CVE-2026-19907	Version corrigee a venir de l'editeur	Desactiver ou mettre a jour le greffon Shipo	9.8
WordPress (greffon AutomatorWP Pro)	Contournement d'autorisation dans le module webhook permettant la reinitialisation du mot de passe de n'importe quel com	14/11/2026	CVE-2026-126173	1.4.4 (corrigee)	Mettre a jour l'extension AutomatorWP Pro	9.8
WordPress (Cloud Storage Manager)	Ecriture arbitraire de fichiers dans le greffon Cloud Storage Manager for Fluent Forms permettant l'execution de code su	14/11/2026	CVE-2026-120522	1.2.0 (corrigee)	Mettre a jour le greffon	9.8
WordPress (coeur)	Execution de code a distance via des chemins de mise a jour previsibles et accessibles depuis le web. Exploitee dans la	31/10/2026	CVE-2026-119977	7.1.4	Mettre a jour WordPress Core	8.1
OpenMage / Magento LTS	Contournement de requete intersites (CSRF) dans les actions OAuth d'administration et de boutique, sans validation du je	13/11/2026	CVE-2026-128049	20.18.2 / 21.0.0-beta3	Mettre a jour OpenMage LTS	9.4
PrestaShop	Controle d'acces defectueux dans l'API Webservice permettant a un detenteur de cle de lire et modifier les clients de to	13/11/2026	CVE-2026-71519	8.2.9 / 9.2.1	Mettre a jour PrestaShop	8.6
SuiteCRM	Injection de code PHP persistante via l'editeur de listes deroulantes Studio, executee avec les droits du serveur web.	05/11/2026	CVE-2026-100358	7.15.2 / 8.10.2	Mettre a jour SuiteCRM	9.4
EspoCRM	XSS stockee dans les articles de base de connaissances permettant a un utilisateur de creer un compte administrateur pie	13/11/2026	CVE-2026-126305	9.3.11 / 10.0.9	Mettre a jour EspoCRM	8.5
Vvveb CMS	Contournement d'authentification par comparaison laxiste dans generateCookie() permettant la prise de controle de compte	13/11/2026	CVE-2026-126377	1.0.9.0	Mettre a jour Vvveb	9.2

II.4 Autres

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS

Vulnerabilite	Description	Date	CVE	Version	Solution	CVSS
Barracuda Email Security Gateway	Contournement d'authentification permettant a un attaquant non authentifie de restaurer une archive de sauvegarde piegee	02/11/2026	CVE-2026-116606	9.4.0.030	Mettre a jour l'appliance Barracuda	9.3
Barracuda (appliances)	Injection de commandes systeme via le champ de configuration du fuseau horaire, executee avec les privileges root. Explo	02/11/2026	CVE-2026-111560	Voir avis editeur	Appliquer le correctif Barracuda	8.6
IBM API Connect	Traversee de repertoire permettant a un attaquant authentifie d'executer du code arbitraire et de realiser des actions a	07/11/2026	CVE-2026-17147	10.0.8.13 / 12.1.1.3	Mettre a jour IBM API Connect	9.9
IBM API Connect	Authentification incorrecte permettant a un attaquant distant d'acceder aux catalogues d'API et aux configurations d'exe	07/11/2026	CVE-2026-17278	12.1.1.3	Mettre a jour IBM API Connect	9.8
Microsoft SharePoint	Autorisation incorrecte permettant a un attaquant authentifie d'elever ses privileges via le reseau.	10/11/2026	CVE-2026-120002	Correctif de novembre 2026	Appliquer les mises a jour SharePoint	9.9
Visual Studio Code	Injection de code permettant a un attaquant non authentifie d'executer du code a distance. Plusieurs autres failles elev	10/11/2026	CVE-2026-120779	Derniere version stable	Mettre a jour Visual Studio Code	9.6
MongoDB Server	Use after free dans le composant de replication, exploitable sans authentification, pouvant provoquer l'arret du serveur	10/11/2026	CVE-2026-118383	Voir avis MongoDB	Mettre a jour MongoDB Server	9.5
SonicWall SonicOS SSLVPN	Contournement des controles d'authentification SAML permettant d'acceder au reseau prive. Exploitee dans la nature selon	06/11/2026	CVE-2026-19868	Voir avis SonicWall	Mettre a jour SonicOS	7.5
Check Point Gaia OS	Le demon DynamicCLI ecoute sur une socket locale accessible en ecriture et sans authentification, permettant a un utilis	12/11/2026	CVE-2026-123039	Voir avis Check Point	Appliquer les correctifs Check Point	7.8
sysPass	Contournement d'authentification permettant de reinstaller une instance deja installee, d'ecraser la configuration et de	13/11/2026	CVE-2026-129110	3.2.12	Mettre a jour sysPass	9.3
WooCommerce (passerelle Sipay)	Absence d'authentification et validation d'integrite insuffisante dans le module de paiement Sipay, expose a la manipula	11/11/2026	CVE-2026-85632	26.9.1	Mettre a jour le module Sipay	9.1
Pillow (libtiff)	Arguments incompatibles transmis a TIFFSetField() dans l'encodeur TIFF, pouvant provoquer un comportement indetermine lo	05/11/2026	CVE-2026-112902	12.3.1	Mettre a jour Pillow	8.3
NocoDB	Elevation de privileges dans initAdminFromEnv.ts : le demarrage du super-administrateur peut etre silencieusement ignore	13/11/2026	CVE-2026-126273	2026.09.0	Mettre a jour NocoDB	9.2
Equipements reseau (D-Link, TP-Link, Edimax)	Multiples debordements de tampon dans les interfaces d'administration web d'equipements de gamme grand public, exploitab	15/11/2026	CVE-2026-129353	Firmware non corrige	Remplacer les equipements en fin de support	9.3

III. Actualites

La Côte d'Ivoire inaugure un centre de cybersécurité à vocation régionale

Abidjan a mis en service un centre de cybersécurité destiné à couvrir l'Afrique de l'Ouest, avec l'appui du groupe Cybastion et de Cisco. L'infrastructure doit permettre aux États de la sous-région de mutualiser la détection d'incidents et la réponse aux attaques, dans un contexte où la plupart des pays ne disposent pas encore de capacités d'analyse 24h/24. Pour le Cameroun, cette initiative illustre une tendance de fond : la mutualisation régionale des moyens devient la seule réponse crédible face à la raréfaction des compétences en cybersécurité.

Source: RFI / Digital Business Africa / Afrique IT News

Interpol : l'intelligence artificielle impliquée dans plus de la moitié de la cybercriminalité africaine

Un rapport d'Interpol indique que l'intelligence artificielle intervient désormais dans plus de la moitié des affaires de cybercriminalité traitées sur le continent. Les groupes criminels l'utilisent pour industrialiser l'ingénierie sociale, générer des messages de hameçonnage en langues locales et automatiser le ciblage des victimes. Les pertes attribuées à la cybercriminalité en Afrique sont estimées à 5 milliards de dollars pour l'année 2025. Le rapport souligne également que les services financiers et le mobile money constituent les secteurs les plus exposés.

Source: Interpol / Planet Biometrics / Agence Ecofin

Smart Africa et e-Crime Bureau signent un protocole d'accord sur la résilience numérique

L'alliance Smart Africa et l'e-Crime Bureau ghanéen ont conclu à Accra un partenariat destiné à renforcer les capacités de prévention et de réponse des États africains. L'accord porte sur la formation des équipes techniques, le partage de renseignements sur les menaces et la mise en commun d'outils de détection. Il s'inscrit dans un mouvement plus large de structuration de la coopération continentale, alors que les attaques par rançongiciel et la fraude en ligne progressent plus vite que les défenses des administrations.

Source: Africa Business Communities / Afriquinfos / Telecompaper

Le mobile money, nouvelle cible privilégiée des cybercriminels en Afrique de l'Ouest

Les opérateurs de transfert d'argent et les acteurs du mobile money, dont Wave, alertent sur la multiplication des fraudes ciblées contre les utilisateurs de services financiers mobiles. Les attaques reposent sur l'usurpation d'identité, le hameçonnage par SMS et l'exploitation de failles dans les interfaces de connexion. Une campagne de sensibilisation a été lancée à Bamako pour appeler à une sécurisation partagée entre opérateurs, banques et autorités de régulation. Le Cameroun, où le mobile money est massivement utilisé, est directement concerné.

Source: Africtelegraph

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.