REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse
Aux Incidents de Sécurité Informatique

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

Bulletin de sécurité N° 1 du mois d'août 2026

Sommaire

I. LEXIQUE DU BULLETIN

Expression	Signification
Date de publication	Date à laquelle la vulnérabilité a été officiellement publiée par le développeur ou constructeur de la ressource concernée.
Dernière version	Lien de téléchargement de la dernière version de la ressource concernée, dans le cas d'une ressource logicielle ou système d'exploitation.
Description	Présentation des détails sur la vulnérabilité, entre autre les versions de la ressource concernée par la vulnérabilité, le vecteur d'exploitation de la vulnérabilité (local, réseau …).
Référence CVE	CVE (Common Vulnerabilities and Exposures) est un annuaire de vulnérabilités de sécurité. Cet annuaire est maintenu par l'organisme MITRE, soutenu par le Département de la Sécurité intérieure des États-Unis. Les identifiants CVE sont des références de la forme CVE-AAAA-NNNN (AAAA est l'année de publication et NNNN un numéro incrémenté). Plus d'information à l'adresse : http://cve.mitre.org/
Score CVSS	CVSS (Common Vulnerability Scoring System) est un système d'évaluation des vulnérabilités qui permet d'associer une valeur (comprise entre 0 et 10) évaluant la criticité d'une vulnérabilité. CVSS fournit un cadre commun pour évaluer les niveaux de criticité, les caractéristiques et les impacts des vulnérabilités de sécurité informatique.
Solution	Lien vers d'éventuelles solutions permettant de colmater ou de contourner la vulnérabilité.
Vulnérabilité	Faille de sécurité publiée, Synopsis de la faille, généralement sur la forme « Vulnérabilité dans X » où X est une ressource informatique, matérielle, logicielle ou système d'exploitation concernée par la vulnérabilité.

II. VULNÉRABILITÉS PUBLIÉES

II.1 NAVIGATEURS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Microsoft Edge	De multiples vulnérabilités ont été découvertes dans HPE Aruba Networking EdgeConnect SD-WAN Orchestrator. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, une atteinte à l'intégrité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • EdgeConnect SD-WAN Orchestrator versions 9.7.0.x antérieures à 9.7.0.43264 • EdgeConnect SD-WAN Orchestrator versions 9.6.3.x antérieures à 9.6.3.40140 • EdgeConnect SD-WAN Orchestrator versions 9.6.2.x antérieures à 9.6.2.40210	04/08/2026	CVE-2026-63456	EdgeConnect SD-WAN Orchestrator versions 9.7.0.... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://csaf.arubanetworking.hpe.com/2026/hpe_aruba_networking_-_hpesbnw05100.txt	**9.8**
Vulnérabilité dans Google Chrome	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Chrome versions antérieures à 151.0.7922.138 pour Mac • Chrome versions antérieures à 151.0.7922.137 pour Windows et Linux • N/A Microsoft Edge versions antérieures à 151.0.4129.86	11/08/2026	CVE-2026-19556	Chrome versions 151.0.7922.138 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01815628406.html	**8.8**
	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants :	06/08/2026	CVE-2026-19165	Chrome versions 151.0.7922.109 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://chromereleases.googleblog.com/2026/08/stable-channel-update-for-desktop_01193673229.html	**7.5**

	• Chrome versions antérieures à 151.0.7922.109 pour Mac • Chrome versions antérieures à 151.0.7922.108 pour Windows et Linux • Microsoft Edge versions antérieures à 151.0.4129.78					
Vulnérabilité dans produits Mozilla	Une vulnérabilité a été découverte dans Mozilla Firefox pour Android. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Firefox pour Android versions antérieures à 153.0.3	04/08/2026	CVE-2026-18809	Firefox pour Android versions 153 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.mozilla.org/en-US/security/advisories/mfsa2026-73/	**6.5**
Vulnérabilité dans Microsoft Edge	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Microsoft Edge versions antérieures à 151.0.4129.59	03/08/2026	CVE-2026-17944	Microsoft Edge versions 151.0.412 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-17915	**4.3**
	De multiples vulnérabilités ont été découvertes dans Microsoft Edge. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Microsoft Edge pour Android versions antérieures à 151.0.4129.59 • Microsoft Edge versions antérieures à 151.0.4129.59	02/08/2026	CVE-2026-17983	Microsoft Edge Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-17670	**4.3**

II.2 SYSTÈMES D'EXPLOITATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Google Android	De multiples vulnérabilités ont été découvertes dans Google Android. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Android toutes versions sans le correctif de sécurité du 3 août 2026	03/08/2026		Android Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/2026/2026-08-01?hl=fr	**NA**
Vulnérabilité dans produits Cisco	De multiples vulnérabilités ont été découvertes dans les produits Cisco. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • NFVIS versions 26.1.x antérieures à 26.1.2 • IOS XE versions 26.1.x antérieures à 26.1.2 • Catalyst SD-WAN versions 26.1.x antérieures à 26.1.2 • Catalyst SD-WAN versions 20.16.x à 20.18.x antérieures à 20.18.4	05/08/2026	CVE-2026-20303	NFVIS versions 26.1.x 26.1.2, IOS... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-bing-MGHrFAkd	**9.9**
Vulnérabilité dans le noyau Linux	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian LTS. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service.	06/08/2026	CVE-2026-64376	Debian LTS 12 bookworm versions antérieures à 6... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-lts-announce/2026/08/msg00007.html	**9.8**

	Les systèmes affectés sont les suivants : • Debian LTS 12 bookworm versions antérieures à 6.12.100-1~deb12u1 • Debian 12 bookworm versions antérieures à 6.1.180-1 • Debian LTS 11 bullseye versions antérieures à 6.1.180-1~deb11u1 • Debian 11 bullseye versions antérieures à 5.10.262-1					
Vulnérabilité dans produits Sophos	Une vulnérabilité a été découverte dans les produits Sophos. Elle permet à un attaquant de provoquer une élévation de privilèges. Les systèmes affectés sont les suivants : • N/A Intercept X Endpoint (Central) versions antérieures à 2026.1.1 pour macOS • N/A Sophos Home versions antérieures à 10.11.6 pour macOS	13/08/2026	CVE-2026-18367	N/A Intercept X Endpoint (Central) Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://sophos.com/en-us/security-advisories/sophos-sa-20260806-ep-macos-lpe	**9.3**
Vulnérabilité dans le noyau Linux	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un déni de service. Les systèmes affectés sont les suivants : • Debian 13 trixie versions antérieures à 6.12.101-1	13/08/2026	CVE-2026-64561	Debian 13 trixie versions 6.12.101-1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00326.html	**8.8**
	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Debian. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à l'intégrité des données et un déni de service. Les systèmes affectés sont les suivants :	06/08/2026	CVE-2026-64552	Debian trixie versions 6.12.100-1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://lists.debian.org/debian-security-announce/2026/msg00316.html	**8.4**

	• Debian trixie versions antérieures à 6.12.100-1					
	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • N/A Red Hat Enterprise Linux for x86_64 10 x86_64 • N/A Red Hat CodeReady Linux Builder for x86_64 10 x86_64 • N/A Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 • N/A Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 • N/A Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64	13/08/2026	CVE-2024-53143	N/A Red Hat Enterprise Linux for x86_64 10 x86_... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:53990	**7.8**
	De multiples vulnérabilités ont été découvertes dans le noyau Linux de Red Hat. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire, une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • Red Hat Enterprise Linux for x86_64 10 x86_64 • Red Hat CodeReady Linux Builder for x86_64 10 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64	06/08/2026	CVE-2026-64531	Red Hat Enterprise Linux for x86_64 10 x86_64,... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://access.redhat.com/errata/RHSA-2026:49033	**7.8**

	• Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64					

Vulnérabilité dans Apple macOS	Une vulnérabilité a été découverte dans Apple macOS. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • macOS Tahoe versions antérieures à 26.6.1 • macOS Sequoia versions antérieures à 15.7.9 • macOS Sonoma versions antérieures à 14.8.9	06/08/2026	CVE-2026-65400	macOS Tahoe versions 26.6.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.apple.com/en-us/148170	**7.1**
Vulnérabilité dans Microsoft Windows	De multiples vulnérabilités ont été découvertes dans Microsoft Windows. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance. Microsoft indique que la vulnérabilité CVE-2026-68820 est activement exploitée. Les systèmes affectés sont les suivants : • N/A Windows Server 2025 (Server Core installation) versions antérieures à 10.0.26100.33296 • N/A Windows Server 2025 versions antérieures à 10.0.26100.33296 • N/A Windows Server 2025 versions antérieures à 10.0.26100.33222 • N/A Windows Server 2025 (Server Core installation) versions antérieures à 10.0.26100.33222 • N/A Windows Server 2022 (Server Core installation) versions antérieures à 10.0.20348.5499	11/08/2026	CVE-2026-59136	N/A Windows Server 2025 (Server Core installati... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62899	**5.5**

Vulnérabilité dans produits Fortinet	De multiples vulnérabilités ont été découvertes dans les produits Fortinet. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • FortiWeb versions 8.0.x antérieures à 8.0.3 • FortiOS versions antérieures à 7.6.7 • FortiWeb versions antérieures à 7.6.7 • FortiProxy versions 7.6.x et antérieures à 7.6.7 • FortiManager versions 7.6.x antérieures à 7.6.2	12/08/2026	CVE-2026-71408	FortiWeb versions 8.0.3 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.fortiguard.com/psirt/FG-IR-26-160	**5.3**

II.3 CMS

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans WordPress	De multiples vulnérabilités ont été découvertes dans WordPress. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • WordPress versions antérieures à 7.0.3	06/08/2026	CVE-2026-64638	WordPress versions 7.0.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://wordpress.org/news/2026/08/wordpress-7-0-3-release/	**NA**
	Une vulnérabilité a été découverte dans WordPress. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes affectés sont les suivants : • WordPress versions antérieures à 7.0.4	12/08/2026	CVE-2026-65640	WordPress versions 7.0.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://wordpress.org/news/2026/08/wordpress-7-0-4-release/	**8.8**

II.4 BASES DE DONNÉES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Nextcloud Mail	De multiples vulnérabilités ont été découvertes dans les produits Nextcloud. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Server versions 34.0.x antérieures à 34.0.1 pour nextcloud • Server versions 33.0.4 à 33.0.x antérieures à 33.0.6 pour nextcloud et nextcloud enterprise • Server versions 32.0.10 à 32.0.x antérieures à 32.0.12 pour nextcloud et nextcloud enterprise • Mail versions 5.7.x antérieures à 5.7.13 • Mail versions 5.6.x antérieures à 5.6.20	05/08/2026	CVE-2026-61545	Server versions 34.0.1 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://github.com/nextcloud/security-advisories/security/advisories/GHSA-99gw-ww6p-f2rr	**NA**
Vulnérabilité dans PostgreSQL	De multiples vulnérabilités ont été découvertes dans PostgreSQL. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • N/A PostgreSQL versions 18.x antérieures à 18.6 • N/A PostgreSQL versions 17.x antérieures à 17.11 • N/A PostgreSQL versions 16.x antérieures à 16.15 • N/A PostgreSQL versions 15.x antérieures à 15.19 • N/A PostgreSQL versions antérieures à 14.24	13/08/2026	CVE-2026-14671	N/A PostgreSQL 18.6 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.postgresql.org/about/news/postgresql-186-1711-1615-1519-1424-and-19-beta-3-released-3365/	**8.8**

II.5 ÉQUIPEMENTS RÉSEAU

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans produits Cisco	Une vulnérabilité a été découverte dans les produits Cisco. Elle permet à un attaquant de provoquer un déni de service à distance. Cisco indique que la vulnérabilité CVE-2026-20349 est activement exploitée. Les systèmes affectés sont les suivants : • Adaptive Security Appliance Adaptative Security Appliance versions 9.24.x antérieures à 9.24.1.221 • Adaptive Security Appliance Adaptative Security Appliance versions 9.23.x antérieures à 9.23.1.211 • Adaptive Security Appliance Adaptative Security Appliance versions 9.22.x antérieures à 9.22.3.191 • Adaptive Security Appliance Adaptative Security Appliance versions 9.20.x antérieures à 9.20.4.235 • Adaptive Security Appliance Adaptative Security Appliance versions 9.18.x sans le correctif 89.18.4.50	11/08/2026	CVE-2026-20349	Adaptive Security Appliance Adaptative Security... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-dzv4mQFF	**8.6**
Vulnérabilité dans Sonicwall Sonicos	Une vulnérabilité a été découverte dans Sonicwall SonicOS. Elle permet à un attaquant de provoquer un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • SonicOS Gen8 Firewalls TZ80, TZ280, TZ280W, TZ380,	05/08/2026	CVE-2026-0516	SonicOS Gen8 Firewalls TZ80, TZ280, TZ280W, TZ3... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0009	**6.5**

	TZ380W, TZ480, TZ580, TZ680, NSa 2800, NSa 3800, NSa 4800 et NSa 5800 versions antérieures à 8.2.2-8015 • SonicOS Gen7 NSv NSv 270, NSv 470 et NSv 870 versions 7.3.3-7015 et antérieures • SonicOS Gen7 NSv NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure) versions 7.3.3-7015 et antérieures • SonicOS Gen7 NSv NSV270, NSv470, NSv870 (ESX, KVM, HYPER-V, AWS, Azure) versions 7.0.1-5169 et antérieures • SonicOS Gen7 NSv NSv 270, NSv 470 et NSv 870 versions 7.0.1-5169 et antérieures					
Vulnérabilité dans Sonicwall Global Vpn Client	Une vulnérabilité a été découverte dans SonicWall Global VPN Client. Elle permet à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : • Global VPN Client versions antérieures à 5.0.0.2008	09/08/2026	CVE-2026-66151	Global VPN Client versions 5.0.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0010	**5.5**

II.6 VIRTUALISATION

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Docker Desktop	Une vulnérabilité a été découverte dans Docker. Elle permet à un attaquant de provoquer une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Docker Desktop versions antérieures à 4.86.0	10/08/2026	CVE-2026-17106	Docker Desktop versions 4.86.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://docs.docker.com/security/security-announcements/#docker-desktop-4860-security-update-cve-2026-17106	**NA**
Vulnérabilité dans VMware	De multiples vulnérabilités ont été découvertes dans VMware Tanzu Greenplum. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Tanzu Greenplum Platform Extension Framework versions antérieures à 8.0.3	09/08/2026	CVE-2026-59921	Tanzu Greenplum Platform Extension Framework Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38158	**5.7**

II.7 SÉCURITÉ

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS
Vulnérabilité dans Tenable Security Center	De multiples vulnérabilités ont été découvertes dans Tenable Security Center. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une injection SQL (SQLi). Les systèmes affectés sont les suivants : • Security Center versions antérieures à 6.9.0	13/08/2026	CVE-2026-19679	Security Center versions 6.9.0 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.tenable.com/security/tns-2026-22	**8.8**
Vulnérabilité dans Clamav	De multiples vulnérabilités ont été découvertes dans ClamAV. Certaines d'entre elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données, un déni de service et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • ClamAV versions 1.5.x antérieures à 1.5.4 • ClamAV versions antérieures à 1.4.6	09/08/2026	CVE-2025-8088	ClamAV versions 1.5.4 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://blog.clamav.net/2026/08/clamav-154-and-146-security-patch.html	**8.8**
Vulnérabilité dans produits Siemens	De multiples vulnérabilités ont été découvertes dans les produits Siemens. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • N/A SIMATIC IoT2050 Advanced with Industrial OS versions antérieures à 4.3.4.1 • N/A Desigo PXC7 versions antérieures à 02.21.194.36-2715 • N/A Desigo PXC5.E24 versions antérieures à 02.21.194.36-2715 • N/A Desigo PXC5.E003 versions antérieures à 02.21.194.36-2715 • N/A Desigo PXC4 versions antérieures à 02.21.194.36-2715	11/08/2026	CVE-2026-59693	N/A SIMATIC IoT2050 Advanced with Industrial OS... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://cert-portal.siemens.com/productcert/html/ssa-781903.html	**4.3**

II.8 AUTRES

Vulnérabilité	Description	Date de publication	Référence CVE	Dernière version	Solution	Score CVSS

Vulnérabilité dans Mattermost	De multiples vulnérabilités ont été découvertes dans les produits Mattermost. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • N/A Mattermost Server versions 11.9.x antérieures à 11.9.1 • N/A Mattermost Server versions 11.8.x antérieures à 11.8.5 • N/A Mattermost Server versions 11.7.x antérieures à 11.7.8 • N/A Mattermost Server versions 10.11.x antérieures à 10.11.23	13/08/2026		N/A Mattermost Server versions 11.9. Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mattermost.com/security-updates/	**NA**
Vulnérabilité dans Wireshark	De multiples vulnérabilités ont été découvertes dans Wireshark. Elles permettent à un attaquant de provoquer un déni de service. Les systèmes affectés sont les suivants : • Wireshark versions 4.6.x antérieures à 4.6.8 • Wireshark versions 4.4.x antérieures à 4.4.18	12/08/2026		Wireshark versions 4.6.8 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.wireshark.org/security/wnpa-sec-2026-71.html	**NA**
Vulnérabilité dans Postfix	De multiples vulnérabilités ont été découvertes dans Postfix. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, un contournement de la politique de sécurité et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Postfix versions 3.11.x antérieures à 3.11.6 • Postfix versions 3.10.x antérieures à 3.10.13 • Postfix versions 3.9.x antérieures à 3.9.14 • Postfix versions 3.8.x antérieures à 3.8.20 • Postfix versions 3.7.x antérieures à 3.7.22	10/08/2026	CVE-2026-43964	Postfix versions 3.11.6 Télécharger	Veuillez-vous référer au Bulletin de sécurité : http://www.postfix.org/announcements/postfix-3.11.6.html	**7.5**

Vulnérabilité dans Cpython	Une vulnérabilité a été découverte dans CPython. Elle permet à un attaquant de provoquer un déni de service à distance. Les systèmes affectés sont les suivants : • CPython sans les derniers correctifs de sécurité	10/08/2026	CVE-2026-18503	CPython sans les derniers correctifs de sécurité Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://mail.python.org/archives/list/security-announce@python.org/thread/KQ7NBMCPAZJHRROQXJQE4GMXGLD5KHBS/	**9.1**
Vulnérabilité dans Openssh	De multiples vulnérabilités ont été découvertes dans OpenSSH. Elles permettent à un attaquant de provoquer un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • OpenSSH versions antérieures à 10.5	10/08/2026	CVE-2026-73281 CVE-2026-73282 CVE-2026-73283	OpenSSH versions 10.5 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.openssh.com/txt/release-10.5	**NA**
Vulnérabilité dans Roundcube Webmail	De multiples vulnérabilités ont été découvertes dans Roundcube. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une atteinte à la confidentialité des données et une falsification de requêtes côté serveur (SSRF). Les systèmes affectés sont les suivants : • Roundcube Webmail versions 1.7.x antérieures à 1.7.3 • Roundcube Webmail versions 1.6.x antérieures à 1.6.18	09/08/2026		Roundcube Webmail Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://roundcube.net/news/2026/08/09/security-updates-1.6.18-and-1.7.3	**NA**
Vulnérabilité dans Veeam One	De multiples vulnérabilités ont été découvertes dans les produits Veeam. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • Veeam ONE versions antérieures à 13.1.0.7034 • Veeam Service Provider Console Service Provider Console versions antérieures à 9.3.0.35057	04/08/2026	CVE-2026-64633	Veeam ONE versions 13.1.0.7034 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.veeam.com/kb4892	**10.0**

Vulnérabilité dans Progress Telerik	De multiples vulnérabilités ont été découvertes dans Progress Telerik. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Telerik UI pour AJAX versions antérieures à 2026.2.708 (2026 Q2 SP1)	06/08/2026	CVE-2026-13187	Telerik UI pour AJAX versions 202 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.telerik.com/products/aspnet-ajax/documentation/knowledge-base/kb-security-rau-padding-oracle-cve-2026-13182	**8.1**
Vulnérabilité dans Check Point	Une vulnérabilité a été découverte dans les produits Check Point. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • Security Management versions R82 antérieures à R82 Take 122 • Multi-Domain Security Management versions R82 antérieures à R82 Take 122 • Security Management versions R82.10 antérieures à R82.10 Take 40 • Multi-Domain Security Management versions R82.10 antérieures à R82.10 Take 40 • Multi-Domain Security Management versions R81.20 antérieures à R81.20 Take 161	03/08/2026	CVE-2026-18574	Security Management versions R82 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://support.checkpoint.com/results/sk/sk185222	**9.3**
Vulnérabilité dans Google Pixel	De multiples vulnérabilités ont été découvertes dans Google Pixel. Elles permettent à un attaquant de provoquer une élévation de privilèges et un problème de sécurité non spécifié par l'éditeur. Les systèmes affectés sont les suivants : • Pixel toutes versions sans le correctif de sécurité du 5 août 2026	04/08/2026	CVE-2026-0163	Pixel toutes versions Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://source.android.com/docs/security/bulletin/pixel/2026/2026-08-01?hl=fr	**9.8**

Vulnérabilité dans Microsoft Azure	De multiples vulnérabilités ont été découvertes dans Microsoft Azure. Elles permettent à un attaquant de provoquer une élévation de privilèges, une atteinte à la confidentialité des données et un contournement de la politique de sécurité. Les systèmes affectés sont les suivants : • N/A Azure Storage Explorer versions antérieures à 20260730.9 • N/A Azure CycleCloud 8.9.2 versions antérieures à 8.9.2 • N/A Azure CycleCloud 8.9.1 versions antérieures à 8.9.1 • N/A Ecesv6-series Azure VM • N/A DCesv6-series Azure VM	11/08/2026	CVE-2026-57104	N/A Azure Storage Explorer Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65806	**8.8**
Vulnérabilité dans Microsoft Office	Une vulnérabilité a été découverte dans Microsoft Office. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance. Les systèmes affectés sont les suivants : • Microsoft Office LTSC 2024 pour éditions 64 bits • Microsoft Office LTSC 2024 pour éditions 32 bits • Microsoft Office LTSC 2021 pour éditions 64 bits • Microsoft Office LTSC 2021 pour éditions 32 bits • Microsoft Office 2019 pour éditions 64 bits	02/08/2026	CVE-2026-62870	Microsoft Office LTSC 2024 pour éditions 64 bit... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62870	**8.8**

Vulnérabilité dans GitLab	De multiples vulnérabilités ont été découvertes dans GitLab. Certaines d'entre elles permettent à un attaquant de provoquer une élévation de privilèges, un déni de service à distance et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) GitLab Community Edition (CE) et Enterprise Edition (EE) versions 19.2.x antérieures à 19.2.2 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) GitLab Community Edition (CE) et Enterprise Edition (EE) versions 19.1.x antérieures à 19.1.4 • GitLab Community Edition (CE) et Gitlab Enterprise Edition (EE) GitLab Community Edition (CE) et Enterprise Edition (EE) versions antérieures à 19.0.6	12/08/2026	CVE-2026-19228	GitLab Community Edition (CE) et Gitlab Enterpr... Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-2-2-released/	**8.5**
Vulnérabilité dans produits Microsoft	De multiples vulnérabilités ont été découvertes dans Microsoft Office. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • N/A Microsoft Office LTSC 2024 pour éditions 64 bits • N/A Microsoft Office LTSC 2024 pour éditions 32 bits • N/A Microsoft Office LTSC pour Mac 2024 versions antérieures à 16.112.26081010 • N/A Microsoft Office LTSC 2021 pour éditions 64 bits • N/A Microsoft Office LTSC 2021 pour éditions 32 bits	11/08/2026	CVE-2026-66807	N/A Microsoft Office LTSC 2024 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63517	**7.8**

	De multiples vulnérabilités ont été découvertes dans les produits Microsoft. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et un déni de service à distance. Les systèmes affectés sont les suivants : • N/A Microsoft Visual Studio 2026 version 18.8 antérieures à 18.8.3 • N/A Microsoft Visual Studio 2022 version 17.14 antérieures à 17.14.38 • N/A Microsoft SharePoint Server 2019 versions antérieures à 16.0.10417.20198 • N/A Microsoft SharePoint Server 2019 versions antérieures à 16.0.10417.20175 • N/A Microsoft Exchange Server 2019 Cumulative Update 15 versions antérieures à 15.02.1748.049	11/08/2026	CVE-2026-59119	N/A Microsoft Visual Studio 2026 version 18.8 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62827	**7.3**

Vulnérabilité dans Sonicwall Email Security	De multiples vulnérabilités ont été découvertes dans les produits SonicWall. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, une élévation de privilèges et une atteinte à la confidentialité des données. Les systèmes affectés sont les suivants : • Email Security versions antérieures à 10.0.36 • N/A GMS versions antérieures à 9.5.2	11/08/2026	CVE-2026-66150	Email Security versions 10.0.36 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0012	**7.8**
Vulnérabilité dans Ivanti Endpoint Manager (Epm)	De multiples vulnérabilités ont été découvertes dans les produits Ivanti. Certaines d'entre elles permettent à un attaquant de provoquer un déni de service à distance, une atteinte à la confidentialité des données et une atteinte à l'intégrité des données. Les systèmes affectés sont les suivants : • Endpoint Manager (EPM) versions antérieures à 2024 SU7 • Neurons for MDM (N-MDM) Neurons pour MDM versions antérieures à R124	11/08/2026	CVE-2026-18127	Endpoint Manager (EPM) Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-August-2026	**7.7**
Vulnérabilité dans Openssl	Une vulnérabilité a été découverte dans OpenSSL. Elle permet à un attaquant de provoquer un déni de service à distance. Les systèmes affectés sont les suivants : • OpenSSL versions 4.0.x antérieures à 4.0.2 • OpenSSL versions 3.6.x antérieures à 3.6.4 • OpenSSL versions 3.5.x antérieures à 3.5.8	13/08/2026	CVE-2026-14456	OpenSSL versions 4.0.2 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://openssl-library.org/news/secadv/20260813.txt	**7.5**

Vulnérabilité dans Synology Assistant	Une vulnérabilité a été découverte dans Synology Assistant. Elle permet à un attaquant de provoquer une atteinte à la confidentialité des données, une atteinte à l'intégrité des données et un déni de service. Les systèmes affectés sont les suivants : • Assistant versions antérieures à 7.0.7-50095	09/08/2026	CVE-2026-4793	Assistant versions 7.0.7-50095 Télécharger	Veuillez-vous référer au Bulletin de sécurité : https://www.synology.com/en-global/security/advisory/Synology_SA_26_12	**7.3**

III. 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 8 n'est plus supporté depuis la fin de l'année 2021. Si votre organisation n'a pas encore effectué une migration vers une version supportée notamment CentOS 8 ou 9 Stream (voir https://www.centos.org/centos-stream/) alors, votre système d'information court de grands risques. En outre, le cycle de vie des versions de CentOS 7 a été prolongé jusqu'en 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 sur celles-ci.

4. Microsoft a mis fin au support de toutes les versions de Windows 7 depuis le 14 janvier 2020. Depuis cette date les systèmes fonctionnant sous Microsoft Windows 7 ne reçoivent plus le support technique, les mises à jour et les correctifs de sécurité. Il est recommandé aux différents Organismes de planifier la migration des postes utilisateurs utilisant encore ce système vers une version supportée de Microsoft Windows, notamment en prenant en compte cette migration dans les prévisions budgétaires. https://support.microsoft.com/fr-ma/help/4057281/windows-7-support-will-end-on-january14-2020

5. Afin de se prémunir au maximum d'éventuelle attaques informatiques pouvant endommager tout ou partie de vos systèmes, vous devez mettre à jour tous vos systèmes et logiciels utilisés. Nous vous recommandons donc de télécharger et d'installer toutes les dernières versions de logiciels et systèmes utilisés, uniquement sur les sites des constructeurs. Car tout logiciel téléchargé d'une source autre que celle du constructeur est potentiellement compromise par des malware et chevaux de Troie.

Par ailleurs, si vous rencontrez quelques difficultés que ce soit dans l'application des correctifs susmentionnés ou ailleurs vous pouvez nous contacter à travers l'adresses email alerts@cirt.antic.cm ou au numéro de téléphone 8202.