ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits de Juniper
Numéro de Référence	60071501/26
Date de Publication	16 Janvier 2026
Risque	Important
Impact	Important

Systèmes affectés

- Junos OS versions 25.2R1-x antérieures à 25.2R1-S2
- Junos OS versions 24.4R2-x antérieures à 24.4R2-S2
- Junos OS versions 24.4R1-x antérieures à 24.4R1-S3
- Junos OS versions 24.2R2-x antérieures à 24.2R2-S3
- Junos OS versions 24.2R1-x antérieures à 24.2R1-S2
- Junos OS versions 23.4R2-x antérieures à 23.4R2-S6
- Junos OS versions 23.4R1-x antérieures à 23.4R1-S2
- Junos OS versions 23.2R2-x antérieures à 23.2R2-S5
- Junos OS versions 22.4R3-x antérieures à 22.4R3-S8
- Junos OS versions 22.3R3-x antérieures à 22.3R3-S4
- Junos OS versions 22.2R3-x antérieures à 22.2R3-S7
- Junos OS versions 21.4R3-x antérieures à 21.4R3-S12
- Junos OS versions 21.2R3-x antérieures à 21.2R3-S10
- Policy Enforcer versions antérieures à 24.1R5
- Policy Enforcer versions antérieures à 24.1R3
- Junos OS Evolved versions 24.4R2-x antérieures à 24.4R2-S1-EVO
- Junos OS Evolved versions 24.2R2-x antérieures à 24.2R2-S3-EVO
- Junos OS Evolved versions 23.4R2-x antérieures à 23.4R2-S6-EVO
- Junos OS Evolved versions 23.2R2-x antérieures à 23.2R2-S5-EVO
- Junos OS Evolved versions 22.4R3-x antérieures à 22.4R3-S9-EVO
- Junos OS Evolved versions 22.3R3-x antérieures à 22.3R3-S3-EVO
- Junos OS Evolved versions 22.2R3-x antérieures à 22.2R3-S4-EVO
- Junos OS Evolved versions 21.4R3-x antérieures à 21.4R3-S7-EVO

Identificateurs externes

CVE-2026-21921 CVE-2026-21920 CVE-2026-21918 CVE-2026-21917 CVE-2026-21914
CVE-2026-21913 CVE-2026-21912 CVE-2026-21911 CVE-2026-21910 CVE-2026-21909
CVE-2026-21908 CVE-2026-21907 CVE-2026-21906 CVE-2026-21905 CVE-2026-21903
CVE-2026-0203 CVE-2025-60011 CVE-2025-60007 CVE-2025-60003 CVE-2025-59961
CVE-2024-50302 CVE-2022-45061 CVE-2021-4189 CVE-2021-3737 CVE-2021-3733
CVE-2021-3177 CVE-2020-8492 CVE-2020-26116 CVE-2019-20907 CVE-2015-20107

Bilan de la vulnérabilité

Juniper annonce la correction de plusieurs vulnérabilités affectant plusieurs versions de ses produits susmentionnés. Un attaquant distant pourrait exploiter ces vulnérabilités pour exécuter du code arbitraire, accéder à des données confidentielles ou causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de Juniper afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire
- Accès à des données confidentielles
- Déni de service

Référence

Bulletins de sécurité Juniper:

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-A-specifically-crafted-show-chassis-command-causes-chassisd-to-crash-CVE-2025-60007
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-EX4000-A-high-volume-of-traffic-destinated-to-the-device-leads-to-a-crash-and-restart-CVE-2026-21913
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-EX4k-Series-QFX5k-Series-In-an-EVPN-VXLAN-configuration-link-flaps-cause-Inter-VNI-traffic-drop-CVE-2026-21910
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Evolved-A-Linux-kernel-vulnerability-in-the-HID-driver-allows-an-attacker-to-read-information-from-

the-HID-Report-buffer-CVE-2024-50302

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Evolved-Flapping-management-interface-causes-MAC-learning-on-label-switched-interfaces-to-stop-CVE-2026-21911
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-MX10k-Series-show-system-firmware-CLI-command-may-lead-to-LC480-or-LC2101-line-card-reset-CVE-2026-21912
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Receipt-of-a-specifically-malformed-ICMP-packet-causes-an-FPC-restart-CVE-2026-0203
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-A-specifically-malformed-GTP-message-will-cause-an-FPC-crash-CVE-2026-21914
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-If-a-specific-request-is-processed-by-the-DNS-subsystem-flowd-will-crash-CVE-2026-21920
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-MX-Series-with-MX-SPC3-or-MS-MPC-Receipt-of-multiple-specific-SIP-messages-results-in-flow-management-process-crash-CVE-2026-21905
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-Specifically-malformed-SSL-packet-causes-FPC-crash-CVE-2026-21917
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-Series-With-GRE-performance-acceleration-enabled-receipt-of-a-specific-ICMP-packet-causes-the-PFE-to-crash-CVE-2026-21906
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-SRX-and-MX-Series-When-TCP-packets-occur-in-a-specific-sequence-flowd-crashes-CVE-2026-21918
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-Subscribing-to-telemetry-sensors-at-scale-causes-all-FPCs-to-crash-CVE-2026-21903
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-BGP-update-with-a-set-of-specific-attributes-causes-rpd-crash-CVE-2025-60003
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Optional-transitive-BGP-attribute-is-modified-before-propagation-to-peers-causing-sessions-to-flap-CVE-2025-60011
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Receipt-of-specific-IS-IS-update-packet-causes-memory-leak-leading-to-RPD-crash-CVE-2026-21909
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Unix-socket-used-to-control-the-jdhcpd-process-is-world-writable-CVE-2025-59961
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-

OS-Evolved-Use-after-free-vulnerability-In-802-1X-authentication-daemon-can-cause-crash-of-the-dot1xd-process-CVE-2026-21908

- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R5-release
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-Space-TLS-SSL-server-supports-use-of-static-key-ciphers-ssl-static-key-ciphers-CVE-2026-21907
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Policy-Enforcer-Multiple-vulnerabilities-in-Python-resolved-in-24-1R3-release
- https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-When-telemetry-collectors-are-frequently-subscribing-and-unsubscribing-to-sensors-chassisd-or-rpd-will-crash-CVE-2026-21921