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	63011004/26
Date de Publication	10 avril 2026
Risque	Important
Impact	Important

Systèmes affectés

- Junos OS versions antérieures à la versipn 23.4R2-S7 sur SRX Series et MX Series
- Junos OS versions 24.4R1 antérieures à la versipn 24.4R1-S3
- SI vLWC versions antérieures à la versipn 3.0.94
- Junos OS Evolved versions 22.2-EVO antérieures à la versipn 22.2R3-S4-EVO sur PTX10004, PTX10008, PTX100016 avec JNP10K-LC1201 ou JNP10K-LC1202
- Junos OS Evolved versions 21.4-EVO antérieures à la versipn 21.4R3-S7-EVO sur PTX10004, PTX10008, PTX100016 avec JNP10K-LC1201 ou JNP10K-LC1202
- Junos OS Evolved versions 24.4R2-EVO antérieures à la versipn 24.4R2-S3-EVO
- Junos OS Evolved versions antérieures à la versipn 21.2R3-S8-EVO sur PTX10004, PTX10008, PTX100016 avec JNP10K-LC1201 ou JNP10K-LC1202
- Junos OS versions 25.2 antérieures à la versipn 25.2R2 sur SRX Series et MX Series
- Junos OS Evolved versions 22.4R3 antérieures à la versipn 22.4R3-S8-EVO
- Junos OS Evolved versions 23.2-EVO antérieures à la versipn 23.2R2-S5-EVO
- Junos OS versions 25.2R2 antérieures à la versipn 25.2R2
- Junos OS versions 23.4 antérieures à la versipn 23.4R2-S7 sur SRX Series
- Junos OS Evolved versions 22.3-EVO antérieures à la versipn 22.3R3-S3-EVO sur PTX10004, PTX10008, PTX100016 avec JNP10K-LC1201 ou JNP10K-LC1202
- Junos OS versions 23.2 antérieures à la versipn 23.2R2-S6 sur SRX Series
- Junos OS versions 24.2R2 antérieures à la versipn 24.2R2-S4
- Junos OS Evolved versions 24.4R1-EVO antérieures à la versipn 24.4R1-S3-EVO
- Junos OS versions 24.2 antérieures à la versipn 24.2R2-S4 sur SRX Series et MX Series
- Junos OS versions 22.2 antérieures à la versipn 22.2R3-S8 sur SRX Series
- Junos OS Evolved versions 25.2R2-EVO antérieures à la versipn 25.2R2-EVO
- Junos OS versions 22.4 antérieures à la versipn 22.4R3-S9 sur SRX Series et MX Series

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Junos OS Evolved versions 23.4-EVO antérieures à la versipn 23.4R2-S8-EVO
- Junos OS Evolved versions 22.4-EVO antérieures à la versipn 22.4R3-S2-EVO sur PTX10004, PTX10008, PTX100016 avec JNP10K-LC1201 ou JNP10K-LC1202
- Junos OS versions 21.2R3 antérieures à la versipn 21.2R3-S10 sur SRX Series
- Junos OS versions 24.4R2 antérieures à la versipn 24.4R2-S3
- Junos OS versions 21.4 antérieures à la versipn 21.4R3-S12 sur SRX Series
- Junos OS Evolved versions 22.4R3 antérieures à la versipn 22.4R3-S9-EVO sur PTX Series
- Junos OS Evolved versions 25.2R1-EVO antérieures à la versipn 25.2R1-S2-EVO
- Junos OS versions antérieures à la versipn 23.2R2-S6 sur SRX Series et MX Series
- Junos OS versions 23.2R2 antérieures à la versipn 23.2R2-S7
- Junos OS versions 22.4 antérieures à la versipn 22.4R3-S9 sur SRX Series
- Junos OS versions 23.4 antérieures à la versipn 23.4R2-S7
- Junos OS versions 22.4R3 antérieures à la versipn 22.4R3-S9
- Junos OS versions 25.2R1 antérieures à la versipn 25.2R1-S2
- Junos OS versions 24.2 antérieures à la versipn 24.2R2-S3 sur SRX Series
- Junos OS Evolved versions 24.2-EVO antérieures à la versipn 24.2R2-S4-EVO
- Junos OS Evolved versions 23.2-EVO antérieures à la versipn 23.2R2-EVO sur PTX10004, PTX10008, PTX100016 avec JNP10K-LC1201 ou JNP10K-LC1202
- Junos OS Evolved versions 23.2-EVO antérieures à la versipn 23.2R2-S6-EVO sur PTX Series

Identificateurs externes

CVE-2022-24805 CVE-2025-13914 CVE-2025-30650 CVE-2026-21915 CVE-2026-21916
CVE-2026-21919 CVE-2026-33771 CVE-2026-33773 CVE-2026-33774 CVE-2026-33775
CVE-2026-33776 CVE-2026-33778 CVE-2026-33779 CVE-2026-33780 CVE-2026-33781
CVE-2026-33782 CVE-2026-33783 CVE-2026-33784 CVE-2026-33785 CVE-2026-33786
CVE-2026-33787 CVE-2026-33788 CVE-2026-33790 CVE-2026-33791 CVE-2026-33797

Bilan de la vulnérabilité

Juniper annonce la correction de plusieurs vulnérabilités affectant plusieurs versions de ses produits susmentionnés. Un attaquant pourrait exploiter ces vulnérabilités pour exécuter du code à distance, accéder à des données confidentielles, contourner des mesures de sécurité, élever ses privilèges 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 à distance
- Contournement de mesures de sécurité
- Elévation de privilèges
- Accès à des données confidentielles
- Déni de service

Référence

Bulletins de sécurité Juniper:

- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Apstra-SSH-host-key-validation-vulnerability-for-managed-devices-CVE-2025-13914
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-CTP-OS-Configuring-password-requirements-does-not-work-which-permits-the-use-of-weak-passwords-CVE-2026-33771
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-JSI-Virtual-Lightweight-Collector-Shell-escape-allows-privilege-escalation-to-root-CVE-2026-21915
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-A-low-privileged-user-can-escalate-their-privileges-so-that-they-can-login-as-root-CVE-2026-21916
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-EX-Series-QFX-Series-If-the-same-egress-filter-is-configured-on-both-an-IRB-and-a-physical-interface-one-of-those-is-not-applied-CVE-2026-33773
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-EX-Series-QFX-Series-In-a-VXLAN-scenario-when-specific-control-protocol-packets-are-received-memory-leaks-and-eventually-no-traffic-is-passed-CVE-2026-33781
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-Evolved-Local-authenticated-attackers-can-gain-access-to-FPCs-CVE-2026-33788
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-Evolved-PTX-Series-If-SRTE-tunnels-provisioned-via-PCEP-are-present-and-specific-gRPC-queries-are-received-evo-aftman-crashes-CVE-2026-33783
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-MX-Series-Firewall-filters-on-lo0-non-0-in-the-default-routing-instance-are-not-in-effect-CVE-2026-33774
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-MX-Series-In-specific-DHCPv6-scenarios-jdhcpd-memory-increases-continuously-with-subscriber-logouts-CVE-2026-33782
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-MX-Series-

Mismatch-between-configured-and-received-packet-types-causes-memory-leak-in-bbe-smgd-CVE-2026-33775

- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-MX-Series-Missing-Authorization-for-specific-request-CLI-commands-in-a-JDM-CSDS-scenario-CVE-2026-33785
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-Privileged-local-user-can-gain-access-to-a-Linux-based-FPC-as-root-CVE-2025-30650
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-SRX-Series-In-a-NAT64-configuration-receipt-of-a-specific-malformed-ICMPv6-packet-will-cause-the-srxpfe-process-to-crash-and-restart-CVE-2026-33790
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-SRX-Series-Insufficient-certificate-verification-for-device-to-SD-cloud-communication-CVE-2026-33779
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-SRX-Series-MX-Series-When-a-specifically-malformed-first-ISAKMP-packet-is-received-kmd-iked-crashes-CVE-2026-33778
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-SRX1500-SRX4100-SRX4200-SRX4600-When-a-specific-show-command-is-executed-chassisd-crashes-CVE-2026-33787
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-SRX1600-SRX2300-SRX4300-When-a-specific-show-command-is-executed-chassisd-crashes-CVE-2026-33786
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-high-frequency-of-connecting-and-disconnecting-netconf-sessions-causes-management-unavailability-CVE-2026-21919
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-attacker-sending-a-specific-genuine-BGP-packet-causes-a-BGP-reset-CVE-2026-33797
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-CVE-2022-24805-resolved-in-net-SNMP
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Execution-of-crafted-CLI-commands-allows-for-arbitrary-shell-injection-as-root-CVE-2026-33791
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-an-EVPN-MPLS-scenario-churn-of-ESI-routes-causes-a-memory-leak-in-l2ald-CVE-2026-33780
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Specific-low-privileged-CLI-command-exposes-sensitive-information-CVE-2026-33776
- https://supportportal.juniper.net/s/article/2026-04-Security-Bulletin-vLWC-Default-

password-is-not-required-to-be-changed-which-allows-unauthorized-high-privileged-access-CVE-2026-33784