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	57340910/25
Date de Publication	09 octobre 2025
Risque	Important
Impact	Important

Systèmes affectés

- Security Director Policy Enforcer versions antérieures à la version 23.1R1 Hotpatch v3
- Junos Space versions antérieures à la version 24.1R4
- Junos Space Security Director versions antérieures à la version 24.1R4
- Junos OS versions antérieures à la version 22.4R3-S8
- Junos OS versions 24.4 antérieures à la version 24.4R2
- Junos OS versions 24.2 antérieures à la version 24.2R2-S1
- Junos OS versions 23.4 antérieures à la version 23.4R2-S5
- Junos OS versions 23.2 antérieures à la version 23.2R2-S4
- Junos OS Evolved versions antérieures à la version 22.4R3-S8-EVO
- Junos OS Evolved versions 24.4-EVO antérieures à la version 24.4R2-EVO
- Junos OS Evolved versions 24.2-EVO antérieures à la version 24.2R2-S2-EVO
- Junos OS Evolved versions 23.4-EVO antérieures à la version 23.4R2-S5-EVO
- Junos OS Evolved versions 23.2-EVO antérieures à la version 23.2R2-S4-EVO

Identificateurs externes

CVE-2015-1427 CVE-2015-3253 CVE-2015-5377 CVE-2018-17244 CVE-2018-17247
CVE-2018-3823 CVE-2018-3824 CVE-2018-3826 CVE-2018-3831 CVE-2019-12900
CVE-2020-11023 CVE-2021-22146 CVE-2021-3903 CVE-2021-40153 CVE-2021-4104
CVE-2021-41043 CVE-2021-41072 CVE-2021-42550 CVE-2021-44228 CVE-2021-44832
CVE-2021-45046 CVE-2021-45105 CVE-2021-47606 CVE-2022-24805 CVE-2022-24806
CVE-2022-24807 CVE-2022-24808 CVE-2022-24810 CVE-2022-48622 CVE-2023-0464
CVE-2023-21102 CVE-2023-2124 CVE-2023-2235 CVE-2023-22655 CVE-2023-25193
CVE-2023-2603 CVE-2023-27349 CVE-2023-28466 CVE-2023-28746 CVE-2023-3090

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

CVE-2023-31248 CVE-2023-32233 CVE-2023-3390 CVE-2023-35001 CVE-2023-35788
CVE-2023-3610 CVE-2023-3776 CVE-2023-38408 CVE-2023-38575 CVE-2023-39368
CVE-2023-4004 CVE-2023-4147 CVE-2023-43490 CVE-2023-43785 CVE-2023-43786
CVE-2023-43787 CVE-2023-44431 CVE-2023-45733 CVE-2023-45866 CVE-2023-46103
CVE-2023-47038 CVE-2023-48161 CVE-2023-4911 CVE-2023-50229 CVE-2023-50230
CVE-2023-51580 CVE-2023-51589 CVE-2023-51592 CVE-2023-51594 CVE-2023-51596
CVE-2023-51764 CVE-2023-52864 CVE-2023-6004 CVE-2023-7104 CVE-2024-12797
CVE-2024-1737 CVE-2024-1975 CVE-2024-21208 CVE-2024-21210 CVE-2024-21217
CVE-2024-21235 CVE-2024-21823 CVE-2024-22025 CVE-2024-2236 CVE-2024-24795
CVE-2024-24806 CVE-2024-2511 CVE-2024-25629 CVE-2024-26327 CVE-2024-26600
CVE-2024-26808 CVE-2024-26828 CVE-2024-26853 CVE-2024-26868 CVE-2024-26897
CVE-2024-27049 CVE-2024-27052 CVE-2024-27065 CVE-2024-27280 CVE-2024-27281
CVE-2024-27282 CVE-2024-27417 CVE-2024-27434 CVE-2024-27982 CVE-2024-27983
CVE-2024-28182 CVE-2024-30203 CVE-2024-30204 CVE-2024-30205 CVE-2024-33621
CVE-2024-34397 CVE-2024-35789 CVE-2024-35800 CVE-2024-35823 CVE-2024-35845
CVE-2024-35848 CVE-2024-35852 CVE-2024-35899 CVE-2024-35911 CVE-2024-35937
CVE-2024-3596 CVE-2024-35969 CVE-2024-36005 CVE-2024-36017 CVE-2024-36020
CVE-2024-36489 CVE-2024-36903 CVE-2024-36921 CVE-2024-36922 CVE-2024-36929
CVE-2024-36941 CVE-2024-36971 CVE-2024-37356 CVE-2024-38428 CVE-2024-38558
CVE-2024-38575 CVE-2024-39487 CVE-2024-39908 CVE-2024-4076 CVE-2024-40928
CVE-2024-40954 CVE-2024-40958 CVE-2024-40961 CVE-2024-41123 CVE-2024-41946
CVE-2024-42934 CVE-2024-43398 CVE-2024-4603 CVE-2024-47538 CVE-2024-47607
CVE-2024-47615 CVE-2024-49761 CVE-2024-52337 CVE-2024-5564 CVE-2024-5742
CVE-2024-6126 CVE-2024-6409 CVE-2024-6655 CVE-2024-8235 CVE-2024-8508
CVE-2024-9632 CVE-2025-0624 CVE-2025-11198 CVE-2025-26594 CVE-2025-26595
CVE-2025-26596 CVE-2025-26597 CVE-2025-26598 CVE-2025-26599 CVE-2025-26600
CVE-2025-26601 CVE-2025-52960 CVE-2025-52961 CVE-2025-59957 CVE-2025-59958
CVE-2025-59962 CVE-2025-59964 CVE-2025-59967 CVE-2025-59968 CVE-2025-59974
CVE-2025-59975 CVE-2025-59976 CVE-2025-59977 CVE-2025-59978 CVE-2025-59980
CVE-2025-59981 CVE-2025-59982 CVE-2025-59983 CVE-2025-59984 CVE-2025-59985
CVE-2025-59986 CVE-2025-59987 CVE-2025-59988 CVE-2025-59989 CVE-2025-59990
CVE-2025-59991 CVE-2025-59992 CVE-2025-59993 CVE-2025-59994 CVE-2025-59995
CVE-2025-59996 CVE-2025-59997 CVE-2025-59998 CVE-2025-59999 CVE-2025-60000
CVE-2025-60001 CVE-2025-60002 CVE-2025-60004 CVE-2025-60006 CVE-2025-60009
CVE-2025-60010

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, élever ses privilèges, contourner des mesures de sécurité 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
- Elévation de privilèges
- Contournement de mesures de sécurité
- Déni de service

Référence

Bulletins de sécurité Juniper:

- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Juniper-Security-Director-Insufficient-authorization-for-sensitive-resources-in-web-interface-CVE-2025-59968
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-EX4600-Series-and-QFX5000-Series-An-attacker-with-physical-access-can-open-a-persistent-backdoor-CVE-2025-59957
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-Flowd-Crash-vulnerability
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-Kernel-memory-disclosure-CVE-2025-60001
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-Multi-Command-Injection-Fixed-CVE-2025-60005
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-Multiple-OS-command-injection-vulnerabilities-fixed-CVE-2025-60006
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-PTX-Series-When-firewall-filter-rejects-traffic-these-packets-are-erroneously-sent-to-the-RE-CVE-2025-59958
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Evolved-PTX-Series-except-PTX10003-An-unauthenticated-adjacent-attacker-sending-specific-valid-traffic-can-cause-a-memory-leak-in-cfmman-leading-to-FPC-crash-and-restart-CVE-2025-52961
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-Multiple-

vulnerabilities-including-RPD-and-FPC-crashes

- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-SRX-Series-BGP-Session-Reset-vulnerability
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-SRX-Series-and-MX-Series-Receipt-of-specific-SIP-packets-in-a-high-utilization-situation-causes-a-flowd-crash-CVE-2025-52960
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-SRX4700-When-forwarding-options-sampling-is-enabled-any-traffic-destined-to-the-RE-will-cause-the-forwarding-line-card-to-crash-and-restart-CVE-2025-59964
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-When-a-user-with-the-name-ftp-or-anonymous-is-configured-unauthenticated-filesystem-access-is-allowed-CVE-2025-59980
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-With-BGP-sharding-enabled-change-in-indirect-next-hop-can-cause-RPD-crash-CVE-2025-59962
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Arbitrary-file-download-vulnerability-in-web-interface-CVE-2025-59976
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Denial-of-Service-vulnerability
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Flooding-device-with-inbound-API-calls-leads-to-WebUI-and-CLI-management-access-DoS-CVE-2025-59975
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R4-release
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Reflected-client-side-HTTP-parameter-pollution-vulnerability-in-web-interface-CVE-2025-59977
- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Security-Director-Policy-Enforcer-An-unrestricted-API-allows-a-network-based-unauthenticated-attacker-to-deploy-malicious-vSRX-images-to-VMWare-NSX-Server-CVE-2025-11198