



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Juniper
Numéro de Référence	44301310/23
Date de Publication	13 Octobre 2023
Risque	Important
Impact	Important

Systemes affectés

- Junos OS Evolved versions antérieures à 20.4R3-S8-EVO, 21.1R3-S2-EVO, 21.2R3-S6-EVO, 21.3R3-S5-EVO, 21.4R3-S5-EVO, 22.1R3-S4-EVO, 22.2R3-S3-EVO, 22.3R3-S1-EVO, 22.4R3-EVO, 23.1R2-EVO, 23.2R1-S1-EVO, 23.2R2-EVO, 23.3R1-EVO
- Junos OS sur les séries MX versions antérieures à 20.4R3-S7, 21.1R3-S5, 21.2R3-S4, 21.3R3-S4, 21.4R3-S3, 22.1R3-S1, 22.2R2-S1, 22.2R3, 22.3R1-S2, 22.3R2, 22.4R1
- Junos OS séries QFX5000 versions antérieures à 20.4R3-S6, 21.1R3-S5, 21.2R3-S5, 21.3R3-S4, 21.4R3-S3, 22.1R3-S2, 22.2R2-S2, 22.2R3, 22.3R2-S1, 22.3R3, 22.4R1-S2, 22.4R2, 23.2R1
- Junos OS versions antérieures à 20.2R3-S6, 20.3R3-S5, 20.4R3-S9, 21.1R3-S5, 21.2R3-S6, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R2-S2, 22.2R3-S2, 22.3R1-S2, 22.3R2-S2, 22.3R3-S1, 22.4R1-S2, 22.4R2-S2, 22.4R3, 23.1R2, 23.2R2, 23.3R1,

Identificateurs externes

- CVE-2022-2097 CVE-2022-2274 CVE-2023-22392 CVE-2023-26551 CVE-2023-26552 CVE-2023-26553 CVE-2023-26554 CVE-2023-26555 CVE-2023-36839 CVE-2023-36841 CVE-2023-36843 CVE-2023-44175 CVE-2023-44176 CVE-2023-44177 CVE-2023-44178 CVE-2023-44181 CVE-2023-44182 CVE-2023-44183 CVE-2023-44184 CVE-2023-44185 CVE-2023-44186 CVE-2023-44187 CVE-2023-44188 CVE-2023-44189 CVE-2023-44190 CVE-2023-44191 CVE-2023-44192 CVE-2023-44193 CVE-2023-44194 CVE-2023-44195 CVE-2023-44196 CVE-2023-44197 CVE-2023-44198 CVE-2023-44199 CVE-2023-44201 CVE-2023-44202 CVE-2023-44203 CVE-2023-44204

Bilan de la vulnérabilité

Juniper annonce la correction de plusieurs vulnérabilités dans les produits susmentionnés. L'exploitation réussie de ces vulnérabilités pourrait permettre à un attaquant de réussir une

élévation de privilèges, de causer un déni de service, de contourner la politique de sécurité et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité Juniper du 11 Octobre 2023 pour plus d'information.

Risque

- Déni de service à distance
- Elévation de privilèges
- Contournement de la politique de sécurité
- Atteinte à la confidentialité de données

Annexe

Bulletin de sécurité Juniper du 11 Octobre 2023 :

- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-and-JunOS-OS-Evolved-Multiple-Vulnerabilities-in-CLI-command>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-and-JunOS-OS-Evolved-Receipt-of-a-specific-genuine-PIM-packet-causes-RPD-crash-CVE-2023-44175>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-QFX5k-12-loop-in-the-overlay-impacts-the-stability-in-a-EVPN-VXLAN-environment-CVE-2023-44181>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-and-JunOS-OS-Evolved-In-a-BGP-scenario-RPD-crashes-upon-receiving-and-processing-a-specific-malformed-ISO-VPN--BGP-UPDATE-packet-CVE-2023-44185>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-and-JunOS-OS-Evolved-High-CPU-load-due-to-specific-NETCONF-command-CVE-2023-44184>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-QFX5000-Series-EX4600-Series-In-a-VxLAN-scenario-an-adjacent-attacker-within-the-VxLAN-sending-genuine-packets-may-cause-a-DMA-memory-leak-to-occur-CVE-2023-44183>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-and-JunOS-OS-Evolved-An-Unchecked-Return-Value-in-multiple-users-interfaces-affects-confidentiality-and-integrity-of-device-operations-CVE-2023-44182>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-and-JunOS-OS-Evolved-RPD-crash-when-attempting-to-send-a-very-long-AS-PATH-to-a-non-4-byte-AS-capable-BGP-neighbor-CVE-2023-44186>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-Evolved-file-copy-CLI-command-can-disclose-password-to-shell-users-CVE-2023-44187>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-jkdsd-crash-due-to-multiple-telemetry-requests-CVE-2023-44188>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-JunOS-OS-Evolved-PTX10003-Series-MAC-address-validation-bypass-vulnerability-CVE-2023-44189>

- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-QFX5000-Series-and-EX4000-Series-Denial-of-Service-DoS-on-a-large-scale-VLAN-due-to-PFE-hogging-CVE-2023-44191>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-Evolved-PTX10001-PTX10004-PTX10008-PTX10016-MAC-address-validation-bypass-vulnerability-CVE-2023-44190>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-QFX5000-Series-DMA-memory-leak-is-observed-when-specific-DHCP-packets-are-transmitted-over-pseudo-VTEP-CVE-2023-44192>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-MX-Series-An-FPC-crash-is-observed-when-CFM-is-enabled-in-a-VPLS-scenario-and-a-specific-LDP-related-command-is-run-CVE-2023-44193>
- <https://supportportal.juniper.net/s/article/2023-10-Security-Bulletin-Junos-OS-An-unauthenticated-attacker-with-local-access-to-the-device-can-create-a-backdoor-with-root-privileges-CVE-2023-44194>