



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans les produits Juniper
<b>Numéro de Référence</b>	44881711/23
<b>Date de Publication</b>	17 Novembre 2023
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- Juniper Secure Analytics (JSA) versions antérieures à 7.5.0 UP7

### Identificateurs externes

- CVE-2020-22218 CVE-2022-44729 CVE-2022-44730 CVE-2023-20593 CVE-2023-20900 CVE-2023-3341 CVE-2023-35788 CVE-2023-3899 CVE-2023-43057

### 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

Veillez se référer au bulletin de sécurité Juniper du 16 Novembre 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 16 Novembre 2023 :

- [https://supportportal.juniper.net/s/article/2023-11-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved?language=en\\_US](https://supportportal.juniper.net/s/article/2023-11-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved?language=en_US)

- <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>