



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits Juniper
Numéro de Référence	39801601/23
Date de Publication	16 Janvier 2023
Risque	Important
Impact	Important

Systemes affectés

- Juniper Networks Junos OS
- Juniper Networks Junos OS Evolved
- Juniper Networks Junos OS on SRX Series
- Juniper Networks Junos OS on vSRX 3.0
- Contrail Service Orchestration
- Juniper Junos OS: QFX10k Series
- Juniper Junos OS Evolved: PTX10003
- Juniper Junos OS: SRX 5000 Series
- Juniper Northstar Controller
- Juniper Junos OS: MX Series
- Juniper Junos OS: ACX2K Series
- Juniper Junos Space
- Contrail Cloud
- Juniper Junos OS: QFX5k Series, EX46xx Series

Identificateurs externes

CVE-2022-22229	CVE-2022-22239	CVE-2022-0778	CVE-2022-3602
CVE-2022-3786	CVE-2023-22414	CVE-2023-22394	CVE-2022-22219
CVE-2023-22397	CVE-2023-22404	CVE-2023-22395	CVE-2023-22417
CVE-2023-22402	CVE-2023-22411	CVE-2023-22391	CVE-2023-22412
CVE-2023-22415	CVE-2023-22401	CVE-2023-22398	CVE-2023-22416
CVE-2023-22408	CVE-2023-22403		

Bilan de la vulnérabilité

Juniper annonce la correction de plusieurs vulnérabilités qui affectent certains de ses produits. Un attaquant distant pourrait exploiter ces failles afin d'exécuter du code arbitraire, injecter du contenu dans une page, accéder à des informations confidentielles ou causer un déni de service.

Solution

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

Risque

- Exécution de code arbitraire à distance.
- Déni de service à distance.
- Injection de contenu dans une page
- Accès à des données confidentielles

Référence

Bulletins de sécurité juniper:

- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-QFX10k-Series-ICCP-flap-will-be-observed-due-to-excessive-specific-traffic-CVE-2023-22403?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-Evolved-PTX10003-An-attacker-sending-specific-genuine-packets-will-cause-a-memory-leak-in-the-PFE-leading-to-a-Denial-of-Service-CVE-2023-22397?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-and-JunOS-Evolved-An-RPD-crash-can-happen-due-to-an-MPLS-TE-tunnel-configuration-change-on-a-directly-connected-router-CVE-2023-22407?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-SRX-Series-MX-Series-with-SPC3-When-an-inconsistent-NAT-configuration-exists-and-a-specific-CLI-command-is-issued-the-SPC-will-reboot-CVE-2023-22409?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Contrail-Service-Orchestration-Multiple-vulnerabilities-resolved-in-CSO-6-3-0?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-SRX-5000-Series-Upon-processing-of-a-specific-SIP-packet-an-FPC-can-crash-CVE-2023-22408?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-and-JunOS-Evolved-A-memory-leak-which-will-ultimately-lead-to-an-rpd-crash-will-be-observed-when-a-peer-interface-flaps-continuously-in-a-Segment-Routing-scenario-CVE-2023-22406?language=en_US

- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Northstar-Controller-Pivotal-RabbitMQ-contains-a-web-management-plugin-that-is-vulnerable-to-a-Denial-of-Service-DoS-attack-CVE-2019-11287?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-QFX10K-Series-PFE-crash-upon-receipt-of-specific-genuine-packets-when-sFlow-is-enabled-CVE-2023-22399?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-SRX-Series-The-flowd-daemon-will-crash-if-SIP-ALG-is-enabled-and-a-malicious-SIP-packet-is-received-CVE-2023-22416?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-and-JunOS-Evolved-RPD-might-crash-when-MPLS-ping-is-performed-on-BGP-LSPs-CVE-2023-22398?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-and-JunOS-Evolved-OpenSSL-Infinite-loop-in-BN-mod-sqrt-reachable-when-parsing-certificates-CVE-2022-0778?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-and-JunOS-Evolved-PTX10008-PTX10016-When-a-specific-SNMP-MIB-is-queried-the-FPC-will-crash-CVE-2023-22401?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-MX-Series-and-SRX-Series-The-flow-processing-daemon-flowd-will-crash-when-a-specific-H-323-packet-is-received-CVE-2023-22415?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-MX-Series-and-SRX-Series-The-flowd-daemon-will-crash-if-the-SIP-ALG-is-enabled-and-specific-SIP-messages-are-processed-CVE-2023-22412?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-SRX-Series-and-MX-Series-Memory-leak-due-to-receipt-of-specially-crafted-SIP-calls-CVE-2023-22394?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-and-JunOS-Evolved-RPD-crash-upon-receipt-of-BGP-route-with-invalid-next-hop-CVE-2023-22393?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-ACX2K-Series-Receipt-of-a-high-rate-of-specific-traffic-will-lead-to-a-Denial-of-Service-DoS-CVE-2023-22391?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-PTX-Series-and-QFX10000-Series-An-FPC-memory-leak-is-observed-when-specific-multicast-packets-are-processed-CVE-2023-22414?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-Space-Multiple-vulnerabilities-resolved-in-22-3R1-release?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-OS-MX-Series-FPC-crash-when-an-IPsec6-tunnel-processes-specific-IPv4-packets-CVE-2023-22413?language=en_US

- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-MX-Series-FPC-crash-when-an-IPsec6-tunnel-processes-specific-IPv4-packets-CVE-2023-22413?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-Evolved-The-kernel-might-restart-in-a-BGP-scenario-where-bgp-auto-discovery-is-enabled-and-such-a-neighbor-flaps-CVE-2023-22402?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-SRX-Series-A-memory-leak-might-be-observed-in-IPsec-VPN-scenario-leading-to-an-FPC-crash-CVE-2023-22417?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-Contrail-Cloud-Multiple-Vulnerabilities-have-been-resolved-in-Contrail-Cloud-release-13-7-0?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-In-an-MPLS-scenario-the-processing-of-specific-packets-to-the-device-causes-a-buffer-leak-and-ultimately-a-loss-of-connectivity-CVE-2023-22395?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-SRX-Series-and-MX-Series-with-SPC3-When-IPsec-VPN-is-configured-iked-will-core-when-a-specifically-formatted-payload-is-received-CVE-2023-22404?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-Evolved-Multiple-vulnerabilities-resolved-in-OpenSSL?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-MX-Series-with-MPC10-MPC11-When-Suspicious-Control-Flow-Detection-scf-d-is-enabled-and-an-attacker-is-sending-specific-traffic-this-causes-a-memory-leak-CVE-2023-22410?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-QFX5k-Series-EX46xx-Series-MAC-limiting-feature-stops-working-after-PFE-restart-device-reboot--CVE-2023-22405?language=en_US
- https://supportportal.juniper.net/s/article/2023-01-Security-Bulletin-JunOS-Receipt-of-crafted-TCP-packets-on-Ethernet-console-port-results-in-MBUF-leak-leading-to-Denial-of-Service-DoS-CVE-2023-22396?language=en_US