ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Juniper
Numéro de Référence	45531201/24
Date de Publication	12 Janvier 2024
Risque	Important
Impact	Important

Systèmes affectés

- CTPView versions versions antérieures à 9.1R5
- Junos OS Evolved version antérieures à 20.4R2-EVO, 20.4R2-S2-EVO, 20.4R3-EVO, 20.4R3-S7-EVO, 21.1R2-EVO, 21.2R2-EVO, 21.2R3-S7-EVO, 21.3R2-EVO, 21.3R3-S5-EVO, 21.4R3-EVO, 21.4R3-S3-EVO, 21.4R3-S5-EVO, 21.4R3-S6-EVO, 22.1R3-EVO, 22.1R3-S2-EVO, 22.1R3-S4-EVO, 22.1R3-S5-EVO, 22.2R2-S1-EVO, 22.2R2-S2-EVO, 22.2R3-EVO, 22.2R3-S2-EVO, 22.2R3-S3-EVO, 22.3R1-EVO, 22.3R2-EVO, 22.3R3-EVO, 22.3R3-S1-EVO, 22.4R1-EVO, 22.4R2-EVO, 22.4R2-S2-EVO, 22.4R3-EVO, 23.1R2-EVO, 23.2R1-EVO, 23.2R1-S1-EVO, 23.2R1-S2-EVO, 23.2R2-EVO, 23.3R1-EVO et 23.4R1-EVO
- Junos OS version antérieures à 20.4R3-S3, 20.4R3-S6, 20.4R3-S7, 20.4R3-S8, 20.4R3-S9, 21.1R3-S4, 21.1R3-S5, 21.2R3, 21.2R3-S3, 21.2R3-S4, 21.2R3-S5, 21.2R3-S6, 21.2R3-S7, 21.3R2-S1, 21.3R3, 21.3R3-S3, 21.3R3-S4, 21.3R3-S5, 21.4R2, 21.4R3, 21.4R3-S3, 21.4R3-S4, 21.4R3-S5, 22.1R2, 22.1R2-S2, 22.1R3, 22.1R3-S1, 22.1R3-S2, 22.1R3-S3, 22.1R3-S4, 22.2R1, 22.2R2, 22.2R2-S1, 22.2R2-S2, 22.2R3, 22.2R3-S1, 22.2R3-S2, 22.2R3-S3, 22.3R1, 22.3R2, 22.3R2-S1, 22.3R2-S2, 22.3R3, 22.3R3-S1, 22.3R3-S2, 22.4R1, 22.4R1-S2, 22.4R2, 22.4R2-S1, 22.4R2-S2, 22.4R3, 23.1R1, 23.1R2, 23.2R1, 23.2R1-S1, 23.2R1-S2, 23.2R2, 23.3R1 et 23.4R1
- Paragon Active Assurance versions antérieures à 3.1.2, 3.2.3, 3.3.2 et 3.4.1
- Security Director Insights versions antérieures à 23.1R1
- Session Smart Router versions antérieures à SSR-6.2.3-r2

Identificateurs externes

- CVE-2016-10009 CVE-2016-2183 CVE-2019-17571 CVE-2020-0465 CVE-2020-0466 CVE-2020-12321 CVE-2020-9493 CVE-2021-0920 CVE-2021-25220 CVE-2021-26341 CVE-2021-26691 CVE-2021-33655 CVE-2021-33656 CVE-2021-34798 CVE-2021-3564 CVE-2021-3573 CVE-2021-3621 CVE-2021-3752 CVE-2021-39275 CVE-2021-4104 CVE-2021-4155 CVE-2021-44228 CVE-2021-44790 CVE-2021-44832 CVE-2022-0330 CVE-2022-0934 CVE-2022-1462 CVE-2022-1679 CVE-2022-1789

CVE-2022-20141 CVE-2022-21699 CVE-2022-2196 CVE-2022-22164 CVE-2022-22942 CVE-2022-23302 CVE-2022-23305 CVE-2022-23307 CVE-2022-25265 CVE-2022-2663 CVE-2022-2795 CVE-2022-2873 CVE-2022-2964 CVE-2022-3028 CVE-2022-30594 CVE-2022-3239 CVE-2022-3524 CVE-2022-3564 CVE-2022-3566 CVE-2022-3567 CVE-2022-3619 CVE-2022-3623 CVE-2022-3625 CVE-2022-3628 CVE-2022-3707 CVE-2022-37434 CVE-2022-38023 CVE-2022-39188 CVE-2022-39189 CVE-2022-41218 CVE-2022-41222 CVE-2022-4129 CVE-2022-4139 CVE-2022-41674 CVE-2022-41973 CVE-2022-41974 CVE-2022-4254 CVE-2022-4269 CVE-2022-42703 CVE-2022-42720 CVE-2022-42721 CVE-2022-42722 CVE-2022-42896 CVE-2022-43750 CVE-2022-4378 CVE-2022-43945 CVE-2022-47929 CVE-2023-0266 CVE-2023-0286 CVE-2023-0386 CVE-2023-0394 CVE-2023-0461 CVE-2023-0767 CVE-2023-1195 CVE-2023-1281 CVE-2023-1582 CVE-2023-1829 CVE-2023-20569 CVE-2023-20593 CVE-2023-2124 CVE-2023-21830 CVE-2023-21843 CVE-2023-21930 CVE-2023-21937 CVE-2023-21938 CVE-2023-21939 CVE-2023-2194 CVE-2023-21954 CVE-2023-21967 CVE-2023-21968 CVE-2023-22045 CVE-2023-22049 CVE-2023-22081 CVE-2023-2235 CVE-2023-22809 CVE-2023-23454 CVE-2023-23918 CVE-2023-23920 CVE-2023-24329 CVE-2023-26464 CVE-2023-2650 CVE-2023-2828 CVE-2023-32067 CVE-2023-32360 CVE-2023-3341 CVE-2023-3446 CVE-2023-36842 CVE-2023-3817 CVE-2023-38408 CVE-2023-38802 CVE-2024-21585 CVE-2024-21587 CVE-2024-21589 CVE-2024-21591 CVE-2024-21594 CVE-2024-21595 CVE-2024-21596 CVE-2024-21597 CVE-2024-21599 CVE-2024-21600 CVE-2024-21601 CVE-2024-21602 CVE-2024-21603 CVE-2024-21604 CVE-2024-21606 CVE-2024-21607 CVE-2024-21611 CVE-2024-21612 CVE-2024-21613 CVE-2024-21614 CVE-2024-21616 CVE-2024-21617

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 10 janvier 2024 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 10 janvier 2024:

- https://supportportal.juniper.net/s/article/2022-01-Security-Bulletin-Junos-OS-Evolved-Telnet-service-may-be-enabled-when-it-is-expected-to-be-disabled-CVE-2022-22164

- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-EX4100-EX4400-EX4600-and-QFX5000-Series-A-high-rate-of-specific-ICMP-traffic-will-cause-the-PFE-to-hang-CVE-2024-21595
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-Evolved-IPython-privilege-escalation-vulnerability-CVE-2022-21699
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-Memory-leak-in-bbe-smgd-process-if-BFD-liveness-detection-for-DHCP-subscribers-is-enabled-CVE-2024-21587
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-5000-Series-Repeated-execution-of-a-specific-CLI-command-causes-a-flowd-crash-CVE-2024-21594
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-specific-BGP-UPDATE-message-will-cause-a-crash-in-the-backup-Routing-Engine-CVE-2024-21596
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-rpd-process-crash-due-to-BGP-flap-on-NSR-enabled-devices-CVE-2024-21585
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-jdhcpd-will-hang-on-receiving-a-specific-DHCP-packet-CVE-2023-36842
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Paragon-Active-Assurance-Control-Center-Information-disclosure-vulnerability-CVE-2024-21589
- https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Session-Smart-Router-Multiple-vulnerabilities-resolved