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	46951504/24
Date de Publication	15 Avril 2024
Risque	Important
Impact	Important

Systèmes affectés

- Cloud Native Router versions antérieures à 23.4
- Junos OS Evolved versions antérieures à 20.4R3-S9-EVO, 21.2R3-S7-EVO, 21.3R3-S5-EVO, 21.4R3-S6-EVO, 22.1R3-S4-EVO, 22.2R3-S2-EVO, 22.3R3-S2-EVO, 22.4R3-EVO, 23.2R2-EVO et 23.4R1-EVO
- Junos OS gamme EX4300 versions antérieures à 20.4R3-S10, 21.2R3-S7 et 21.4R3-S6
- Junos OS gamme EX9200-15C versions antérieures à 21.2R3-S1, 21.4R3, 22.1R2 et 22.2R2
- Junos OS gamme SRX 5000 Series avec SPC2 versions antérieures à 21.2R3-S7, 21.4, 22.1, 22.2, 22.3, 22.4 et 23.2
- Junos OS gammes ACX5448 et ACX710 versions antérieures à 20.4R3-S9, 21.2R3-S5, 21.3R3-S5, 21.4R3-S4, 22.1R3-S2, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2 et 23.2R1
- Junos OS gammes MX Series avec SPC3 et MS-MPC versions antérieures à 21.2R3-S6, 21.3R3-S5, 21.4R3-S5, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3 et 23.2R1
- Junos OS gammes MX Series versions antérieures à 20.4R3-S5, 21.1, 21.2R3-S1, 21.3, 21.4R3, 22.1R2, 22.2R2 et 22.3
- Junos OS gammes QFX5000 Series, EX4400 Series, EX4100 Series et EX4650 Series versions antérieures à 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S4, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3 et 23.2R1
- Junos OS gammes SRX Branch Series versions antérieures à 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 et 23.2R1
- Junos OS gammes SRX4600 versions antérieures à 21.2R3-S7, 21.4R3-S6, 22.1R3-S5, 22.2R3-S3, 22.3R3-S2, 22.4R3, 23.2R1-S2, 23.2R2 et 23.4R1
- Junos OS versions antérieures à 20.4R3-S9, 21.1R3, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5,

22.1R3-S4, 22.2R3-S2, 22.3R3-S2, 22.4R3 et 23.4R2
- Paragon Active Assurance versions antérieures à 4.2.1
- Paragon Active Assurance versions antérieures à 4.3.0
- cRPD versions antérieures à 23.4R1

Identificateurs externes

CVE-2011-1089 CVE-2011-1675 CVE-2011-1676 CVE-2011-1677 CVE-2016-10009
CVE-2016-2781 CVE-2017-18018 CVE-2018-1000120 CVE-2018-1000122
CVE-2018-1000215 CVE-2018-1000654 CVE-2018-20225 CVE-2018-20482
CVE-2018-7738 CVE-2019-17041 CVE-2019-17042 CVE-2019-18276 CVE-2019-9923
CVE-2020-14343 CVE-2020-1747 CVE-2020-19185 CVE-2020-19186 CVE-2020-19187
CVE-2020-19188 CVE-2020-19189 CVE-2020-19190 CVE-2020-22916 CVE-2020-25659
CVE-2020-27350 CVE-2020-27783 CVE-2020-28493 CVE-2020-28928 CVE-2020-36242
CVE-2020-8037 CVE-2020-8284 CVE-2020-8285 CVE-2020-8286 CVE-2021-20193
CVE-2021-22946 CVE-2021-22947 CVE-2021-23240 CVE-2021-28831 CVE-2021-28957
CVE-2021-30139 CVE-2021-33560 CVE-2021-34434 CVE-2021-36159 CVE-2021-37600
CVE-2021-39531 CVE-2021-39533 CVE-2021-39534 CVE-2021-40528 CVE-2021-41039
CVE-2022-2795 CVE-2022-3996 CVE-2022-4304 CVE-2022-4450 CVE-2022-48522
CVE-2022-48554 CVE-2023-0215 CVE-2023-0216 CVE-2023-0217 CVE-2023-0286
CVE-2023-0401 CVE-2023-0466 CVE-2023-0809 CVE-2023-1428 CVE-2023-2253
CVE-2023-23914 CVE-2023-23915 CVE-2023-23931 CVE-2023-2603 CVE-2023-2650
CVE-2023-27043 CVE-2023-28366 CVE-2023-29491 CVE-2023-32681 CVE-2023-32731
CVE-2023-32732 CVE-2023-3446 CVE-2023-3592 CVE-2023-36054 CVE-2023-38408
CVE-2023-38545 CVE-2023-38546 CVE-2023-3978 CVE-2023-39975 CVE-2023-40217
CVE-2023-41913 CVE-2023-43804 CVE-2023-44487 CVE-2023-46218 CVE-2023-4785
CVE-2023-4806 CVE-2023-4807 CVE-2023-48795 CVE-2023-49083 CVE-2023-5156
CVE-2023-5981 CVE-2024-30378 CVE-2024-30380 CVE-2024-30381 CVE-2024-30382
CVE-2024-30384 CVE-2024-30386 CVE-2024-30387 CVE-2024-30388 CVE-2024-30389
CVE-2024-30390 CVE-2024-30391 CVE-2024-30392 CVE-2024-30394 CVE-2024-30395
CVE-2024-30397 CVE-2024-30398 CVE-2024-30401 CVE-2024-30402 CVE-2024-30403
CVE-2024-30405 CVE-2024-30406 CVE-2024-30407 CVE-2024-30409 CVE-2024-30410

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 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

- Déni de service
- Exécution de code arbitraire

Référence

Bulletins de sécurité juniper:

- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Juniper-Cloud-Native-Router-Multiple-vulnerabilities-resolved-in-23-4-release?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-A-specific-EVPN-type-5-route-causes-rpd-crash-CVE-2024-30394?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-ACX5448-ACX710-Due-to-the-interface-flaps-the-PFE-process-can-crash-CVE-2024-30387?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-An-invalid-certificate-causes-a-Denial-of-Service-in-the-Internet-Key-Exchange-IKE-process-CVE-2024-30397?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-EX4300-Series-Firewall-filter-not-blocking-egress-traffic-CVE-2024-30389?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-EX4300-Series-If-a-specific-CLI-command-is-issued-PFE-crashes-will-occur-CVE-2024-30384?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-EX4300-Series-Loopback-filter-not-blocking-traffic-despite-having-discard-term-CVE-2024-30410?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-Evolved-ACX-Series-with-Paragon-Active-Assurance-Test-Agent-A-local-high-privileged-attacker-can-recover-other-administrators-credentials-CVE-2024-30406?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-Evolved-Connection-limits-is-not-being-enforced-while-the-resp-rate-limit-is-being-enforced-CVE-2024-30390?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-Evolved-When-MAC-learning-happens-and-an-interface-gets-flapped-the-PFE-crashes-CVE-2024-30403?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-Evolved-

libslax-Multiple-vulnerabilities-in-libslax-resolved?language=en_US

- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-MX-Series-and-EX9200-15C-Stack-based-buffer-overflow-in-aftman-CVE-2024-30401?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-MX-Series-bbe-smgd-process-crash-upon-execution-of-specific-CLI-commands-CVE-2024-30378?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-MX-Series-with-SPC3-and-MS-MPC-MIC-When-URL-filtering-is-enabled-and-a-specific-URL-request-is-received-a-flowd-crash-occurs-CVE-2024-30392?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-MX-Series-with-SPC3-and-SRX-Series-When-IPsec-authentication-is-configured-with-hmac-sha-384-and-hmac-sha-512-no-authentication-of-traffic-is-performed-CVE-2024-30391?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-QFX5000-Series-and-EX-Series-Specific-malformed-LACP-packets-will-cause-flaps-CVE-2024-30388?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-SRX-Branch-Series-When-DNS-proxy-is-configured-and-specific-DNS-queries-are-received-resolver-s-performance-is-degraded-CVE-2022-2795?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-SRX4600-Series-A-high-amount-of-specific-traffic-causes-packet-drops-and-an-eventual-PFE-crash-CVE-2024-30398?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-malformed-BGP-tunnel-encapsulation-attribute-will-lead-to-an-rpd-crash-CVE-2024-30395?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Higher-CPU-consumption-on-routing-engine-leads-to-Denial-of-Service-DoS-CVE-2024-30409?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-EVPN-VXLAN-scenario-state-changes-on-adjacent-systems-can-cause-an-l2ald-process-crash-CVE-2024-30386?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Junos-OS-and-Junos-OS-Evolved-RPD-crash-when-CoS-based-forwarding-CBF-policy-is-configured-CVE-2024-30382?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-cURL-vulnerabilities-resolved?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-The-l2ald-crashes-on-receiving-telemetry-messages-from-a-specific-subscription-CVE-2024-30402?language=en_US

- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-l2cpd-crash-upon-receipt-of-a-specific-TLV-CVE-2024-30380?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Paragon-Active-Assurance-probe-serviced-exposes-internal-objects-to-local-users-CVE-2024-30381?language=en_US
- https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-cRPD-Multiple-vulnerabilities-resolved-in-23-4R1-release?language=en_US