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 des produits Juniper
Numéro de Référence	41371404/23
Date de Publication	14 Avril 2023
Risque	Important
Impact	Important

Systèmes affectés

- Juniper Secure Analytics (JSA) avec Networks Security Threat Response Manager (STRM) versions antérieures à la version 7.5.0UP4
- JunosOS Evolved versions antérieures à la version 20.1R3-EVO, 20.2R2-EVO, 20.3R2-EVO, 20.4R1-EVO, 20.4R3-S5-EVO, 20.4R3-S6-EVO, 20.4R3-S7-EVO, 21.1R3-S4-EVO, 21.2R3-EVO, 21.2R3-S4-EVO, 21.2R3-S5-EVO, 21.3R2-EVO, 21.3R3-EVO, 21.3R3-S1-EVO, 21.4R1-EVO, 21.4R1-S2-EVO, 21.4R2-EVO, 21.4R2-S1-EVO, 21.4R3-EVO, 21.4R3-S1-EVO, 22.1R1-EVO, 22.1R2-EVO, 22.1R3-EVO, 22.2R1-EVO, 22.2R2-EVO et 22.3R1-EVO
- JunosOS versions antérieures à la version 18.1R3-S11, 18.2R3-S6, 18.3R3-S4, 18.4R3-S6, 19.1R3-S4, 19.2R3-S1, 19.2R3-S7, 19.3R3-S1, 19.3R3-S7, 19.3R3-S8, 19.4R3, 19.4R3-S10, 19.4R3-S11, 19.4R3-S12, 19.4R3-S9, 20.1R2, 20.2R2, 20.2R3-S5, 20.2R3-S6, 20.2R3-S7, 20.3R1-S1, 20.3R2, 20.3R3-S2, 20.3R3-S5, 20.3R3-S6, 20.4R1, 20.4R3-S3, 20.4R3-S4, 20.4R3-S5, 20.4R3-S6, 20.4R3-S7, 21.1R3, 21.1R3-S3, 21.1R3-S4, 21.1R3-S5, 21.2R3, 21.2R3-S2, 21.2R3-S3, 21.2R3-S4, 21.3R2, 21.3R3, 21.3R3-S1, 21.3R3-S2, 21.3R3-S3, 21.4R1, 21.4R2, 21.4R2-S1, 21.4R3, 21.4R3-S1, 21.4R3-S2, 21.4R3-S3, 22.1R1, 22.1R2, 22.1R2-S1, 22.1R2-S2, 22.1R3, 22.1R3-S1, 22.2R1, 22.2R1-S2, 22.2R2, 22.2R2-S1, 22.2R2-S2, 22.2R3, 22.3R1, 22.3R1-S1, 22.3R1-S2, 22.3R2, 22.4R1, 22.4R1-S1, 22.4R2 et 23.1R1
- Paragon Active Assurance versions antérieures à la version 4.1.2

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Identificateurs externes

CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824
CVE-2022-22825 CVE-2022-22826 CVE-2022-22827 CVE-2022-23852 CVE-2022-23990
CVE-2022-25235 CVE-2022-25236 CVE-2022-25313 CVE-2022-25314 CVE-2022-25315
CVE-2022-42889 CVE-2023-1697 CVE-2023-28959 CVE-2023-28960 CVE-2023-28961
CVE-2023-28962 CVE-2023-28963 CVE-2023-28964 CVE-2023-28965 CVE-2023-28966
CVE-2023-28967 CVE-2023-28968 CVE-2023-28970 CVE-2023-28971 CVE-2023-28972
CVE-2023-28973 CVE-2023-28974 CVE-2023-28975 CVE-2023-28976 CVE-2023-28978
CVE-2023-28979 CVE-2023-28980 CVE-2023-28981 CVE-2023-28982 CVE-2023-28983
CVE-2023-28984

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

Veuillez 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/2023-04-Security-Bulletin-JSA-Series-Apache-Commons-Text-prior-to-1-10-0-allows-RCE-when-applied-to-untrusted-input-due-to-insecure-interpolation-defaults-CVE-2022-42889
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-ACX-Series-IPv6-firewall-filter-is-not-installed-in-PFE-when-from-next-header-ah-is-used-CVE-2023-28961
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Docker-repository-is-world-writeable-allowing-low-privileged-local-user-to-inject-files-into-Docker-containers-CVE-2023-28960
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-

Local-low-privileged-user-with-shell-access-can-execute-CLI-commands-as-root-CVE-2023-28966

- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Read-access-to-some-confidential-user-information-is-possible-CVE-2023-28978
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-Shell-Injection-vulnerability-in-the-gNOI-server-CVE-2023-28983
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Evolved-The-sysmanctl-shell-command-allows-a-local-user-to-gain-access-to-some-administrative-actions-CVE-2023-28973
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-In-a-6PE-scenario-upon-receipt-of-a-specific-IPv6-packet-an-integrity-check-fails-CVE-2023-28979
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-JRR200-Kernel-crash-upon-receipt-of-a-specific-packet-CVE-2023-28970
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-MX-Series-If-a-specific-traffic-rate-goes-above-the-DDoS-threshold-it-will-lead-to-an-FPC-crash-CVE-2023-28976
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-MX-Series-In-a-BBE-scenario-upon-receipt-of-specific-malformed-packets-from-subscribers-the-process-bbe-smgd-will-crash-CVE-2023-28974
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-J-Web
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-Multiple-vulnerabilities-in-expat-resolved
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-NFX-Series-set-system-ports-console-insecure-allows-root-password-recovery-CVE-2023-28972
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX-Series-The-PFE-may-crash-when-a-lot-of-MAC-addresses-are-being-learned-and-aged-CVE-2023-28984
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX10000-Series-PTX1000-Series-The-dcpfe-process-will-crash-when-a-malformed-ethernet-frame-is-received-CVE-2023-1697
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX10002-Failure-of-storm-control-feature-may-lead-to-Denial-of-Service-CVE-2023-28965
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-QFX10002-PFE-wedges-and-restarts-upon-receipt-of-specific-malformed-packets-CVE-2023-28959
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-SRX-Series-Policies-that-rely-on-JDPI-Decoder-actions-may-fail-open-CVE-2023-28968
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-The-kernel-will-crash-when-certain-USB-devices-are-inserted-CVE-2023-28975

- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-attacker-sending-genuine-BGP-packets-causes-an-RPD-crash-CVE-2023-28967
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-If-malformed-IPv6-router-advertisements-are-received-memory-corruption-will-occur-which-causes-an-rpd-crash-CVE-2023-28981
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BGP-rib-sharding-scenario-an-rpd-crash-will-happen-shortly-after-a-specific-CLI-command-is-issued-CVE-2023-28980
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-BGP-rib-sharding-scenario-when-a-route-is-frequently-updated-an-rpd-memory-leak-will-occur-CVE-2023-28982
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Malformed-BGP-flowspec-update-causes-RPD-crash-CVE-2023-28964
- https://supportportal.juniper.net/s/article/2023-04-Security-Bulletin-Paragon-Active-Assurance-Enabling-the-timescaledb-enables-IP-forwarding-CVE-2023-28971