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 Juniper Junos OS
Numéro de Référence	42871407/23
Date de Publication	14 Juillet 2023
Risque	Important
Impact	Important

Systèmes affectés

- Juniper Networks Contrail Cloud versions antérieures à 16.3.0
- Juniper Networks Junos Space versions antérieures à 23.1R1
- Juniper Networks gammes SRX et MX versions antérieures à SigPack 3598
- Junos OS Evolved versions antérieures à 20.4R3-S6-EVO, 20.4R3-S7-EVO, 21.2R3-S5-EVO, 21.3R3-S1-EVO, 21.3R3-S4-EVO, 21.4R3-EVO, 21.4R3-S2-EVO, 21.4R3-S3-EVO, 21.4R3-S4-EVO, 22.1R1-S2-EVO, 22.1R2-EVO, 22.1R3-EVO, 22.1R3-S3-EVO, 22.2R2-EVO, 22.2R2-S1-EVO, 22.2R3-S2-EVO*, 22.2R3-EVO et 22.3R1-EVO, 22.3R2-EVO, 22.3R3-EVO, 22.4R1-EVO, 22.4R1-S2-EVO, 22.4R2-EVO, 23.1R1-EVO
- Junos OS gamme MX versions antérieures à 19.1R3-S10, 19.2R3-S7, 19.3R3-S8, 19.4R3-S12, 20.2R3-S8, 20.4R3-S7, 21.1R3-S5, 21.2R3-S5, 21.2R3-S4, 21.3R3-S4, 21.4R3-S3, 21.4R3-S4, 22.1R3-S2, 22.1R3-S3, 22.2R3-S1, 22.3R3, 22.3R2-S1, 22.4R1-S2, 22.4R2 et 23.1R1
- Junos OS gamme QFX10000 versions antérieures à 20.4R3-S5, 21.1R3-S5, 21.2R3-S5, 21.3R3-S4, 21.4R3-S1, 22.1R3, 22.2R2, 22.3R1-S2, 22.3R2 et 22.4R1
- Junos OS gamme SRX versions antérieures à 20.2R3-S7, 20.4R3-S6, 21.1R3-S5, 21.2R3-S4, 21.3R3-S4, 21.4R3-S3, 22.1R3-S1, 22.2R3, 22.3R2, 22.3R2-S1, 22.3R3, 22.4R1-S1, 22.4R1-S2, 22.4R2 et 23.1R1
- Junos OS gammes SRX 4600 et SRX 5000 versions antérieures à 20.2R3-S7, 20.4R3-S7, 21.1R3-S5, 21.2R3-S3, 21.3R3-S3, 21.4R3-S1, 22.1R3, 22.2R2, 22.3R1-S1, 22.3R2 et 22.4R1
- Junos OS versions antérieures à 19.1R3-S10, 19.2R3-S7, 19.3R3-S7, 19.3R3-S8, 19.4R3-S9, 19.4R3-S10, 19.4R3-S11, 20.2R3-S7, 20.3R3-S5, 20.3R3-S6, 20.4R3-S6, 20.4R3-S7, 21.1R3-S4, 21.2R3-S2, 21.3R3-S1, 21.4R3, 22.1R1-S2, 22.1R2, 22.2R2, 20.2R3-S6, 20.4R3-S5, 21.1R3-S4, 21.2R3-S3, 21.2R3-S5, 21.3R3-S2, 21.3R3-S4, 21.4R3, 21.4R3-S4,

22.1R3, 22.2R2, 22.2R3, 22.3R1, 22.3R2, 22.4R1 et 23.2R1

Identificateurs externes

CVE-2017-7653 CVE-2017-7654 CVE-2017-7655 CVE-2019-11358 CVE-2020-11868
CVE-2020-13817 CVE-2020-13946 CVE-2020-7071 CVE-2021-21702 CVE-2021-21703
CVE-2021-21704 CVE-2021-21705 CVE-2021-21707 CVE-2021-21708 CVE-2021-25220
CVE-2021-26401 CVE-2021-40085 CVE-2022-23825 CVE-2022-2588 CVE-2022-26373
CVE-2022-2795 CVE-2022-2964 CVE-2022-29900 CVE-2022-29901 CVE-2022-30123
CVE-2022-31625 CVE-2022-31626 CVE-2022-31627 CVE-2022-31628 CVE-2022-31629
CVE-2022-3276 CVE-2022-38023 CVE-2022-41974 CVE-2022-42703 CVE-2022-42898
CVE-2022-4378 CVE-2023-28985 CVE-2023-36831 CVE-2023-36832 CVE-2023-36833
CVE-2023-36834 CVE-2023-36835 CVE-2023-36836 CVE-2023-36838 CVE-2023-36840
CVE-2023-36848 CVE-2023-36849 CVE-2023-36850

Bilan de la vulnérabilité

Juniper annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées de son système d'exploitation Junos OS. Un attaquant distant non authentifié pourrait exploiter ces vulnérabilités pour exécuter du code arbitraire, contourner de mesures de sécurité ou causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité de Juniper afin d'installer les nouvelles mises à jour.

Risque

- Déni de service
- Exécution de code arbitraire
- Contournement de mesures de sécurité

Référence

Bulletins de sécurité juniper:

- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Contrail-Cloud-Multiple-Vulnerabilities-have-been-resolved-in-Contrail-Cloud-release-16-3-0?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-Evolved-Multiple-NTP-vulnerabilities-resolved?language=en_US

- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-Evolved-PTX10001-36MR-and-PTX10004-PTX10008-PTX10016-with-LC1201-1202-The-aftman-bt-process-will-crash-in-a-MoFRR-scenario-CVE-2023-36833?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-J-Web-Multiple-Vulnerabilities-in-PHP-software?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-MX-Series-An-MPC-will-crash-upon-receipt-of-a-malformed-CFM-packet-CVE-2023-36850?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-MX-Series-PFE-crash-upon-receipt-of-specific-packet-destined-to-an-AMS-interface-CVE-2023-36832?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-QFX10000-Series-All-traffic-will-be-dropped-after-a-specific-valid-IP-packet-has-been-received-which-needs-to-be-routed-over-a-VXLAN-tunnel-CVE-2023-36835?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-4600-and-SRX-5000-Series-The-receipt-of-specific-genuine-packets-by-SRXes-configured-for-L2-transparency-will-cause-a-DoS-CVE-2023-36834?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-Series-A-flowd-core-occurs-when-running-a-low-privileged-CLI-command-CVE-2023-36838?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-SRX-Series-jbuf-memory-leak-when-SSL-Proxy-and-UTM-Web-Filtering-is-applied-CVE-2023-36831?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-The-FPC-will-crash-on-receiving-a-malformed-CFM-packet-CVE-2023-36848?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-An-rpd-crash-occurs-when-a-specific-L2VPN-command-is-run-CVE-2023-36840?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-MoFRR-scenario-an-rpd-core-may-be-observed-when-a-low-privileged-CLI-command-is-executed-CVE-2023-36836?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-vulnerabilities-have-been-resolved-in-MQTT?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-The-l2cpd-will-crash-when-a-malformed-LLDP-packet-is-received-CVE-2023-36849?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-23-1R1-release?language=en_US
- https://supportportal.juniper.net/s/article/2023-07-Security-Bulletin-SRX-Series-and-MX-Series-An-FPC-core-is-observed-when-IDP-is-enabled-on-the-device-and-a-specific-

malformed-SSL-packet-is-received-CVE-2023-28985?language=en_US

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