



BULLETIN DE SECURITE

Titre	Vulnérabilité dans les produits Juniper
Numéro de Référence	49461309/24
Date de Publication	13 Septembre 2024
Risque	Important
Impact	Important

Systemes affectés

- Junos OS versions antérieures à 20.4R3-S10
- Junos OS versions 23.2 antérieures à 23.2R2
- Junos OS versions 22.4 antérieures à 22.4R3
- Junos OS versions 22.3 antérieures à 22.3R3-S1
- Junos OS versions 22.2 antérieures à 22.2R3-S3
- Junos OS versions 22.1 antérieures à 22.1R3-S4
- Junos OS versions 21.4 antérieures à 21.4R3-S7
- Junos OS versions 21.3 antérieures à 21.3R3-S5
- Junos OS versions 21.2 antérieures à 21.2R3-S5
- Junos OS versions 21.1R1*
- Junos OS Evolved versions antérieures à 20.4R3-S10-EVO
- Junos OS Evolved versions 23.2-EVO antérieures à 23.2R2-EVO
- Junos OS Evolved versions 22.4-EVO antérieures à 22.4R3-EVO
- Junos OS Evolved versions 22.3-EVO antérieures à 22.3R3-S1-EVO
- Junos OS Evolved versions 22.2-EVO antérieures à 22.2R3-S3-EVO
- Junos OS Evolved versions 22.1-EVO antérieures à 22.1R3-S4-EVO
- Junos OS Evolved versions 21.4-EVO antérieures à 21.4R3-S5-EVO
- Junos OS Evolved versions 21.3-EVO antérieures à 21.3R3-S5-EVO
- Junos OS Evolved versions 21.2-EVO antérieures à 21.2R3-S7-EVO

Identificateurs externes

- CVE-2023-4481

Bilan de la vulnérabilité

Juniper annonce la correction d'une vulnérabilité dans les versions susmentionnées de Junos OS et Junos OS Evolved. L'exploitation de cette faille peut permettre à un attaquant de causer un déni de service à distance.

Solution

Veillez se référer au bulletin de sécurité Juniper du 12 Septembre 2024 pour plus d'information.

Risque

- Déni de service à distance

Annexe

Bulletin de sécurité Juniper du 12 Septembre 2024:

- <https://supportportal.juniper.net/s/article/2023-08-29-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-crafted-BGP-UPDATE-message-allows-a-remote-attacker-to-de-peer-reset-BGP-sessions-CVE-2023-4481>