



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans Juniper Junos OS
<b>Numéro de Référence</b>	47371305/24
<b>Date de Publication</b>	13 Mai 2024
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- Junos OS versions 23.2 antérieures à 23.2R1-S1 et 23.2R2
- Junos OS versions 22.4R1 antérieures à 22.4R2-S2 et 22.4R3
- Junos OS versions 22.3R3 antérieures à 22.3R3-S1
- Junos OS versions 22.3R1 antérieures à 22.3R2-S2
- Junos OS versions 22.2R2 antérieures à 22.2R3-S2
- Junos OS versions 21.4R3 antérieures à 21.4R3-S5
- Junos OS et Junos OS Evolved avec OpenSSH versions antérieures à 9.6

### Identificateurs externes

- CVE-2016-10009 CVE-2020-1628 CVE-2023-44186 CVE-2023-44188 CVE-2023-48795 CVE-2024-21612 CVE-2024-21617

### Bilan de la vulnérabilité

Juniper a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités affectant Junos OS. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire à distance, de réussir une élévation de privilèges, de causer un déni de service et de porter atteinte à la confidentialité de données.

### Solution

Veuillez se référer au bulletin de sécurité Juniper pour plus d'information.

### Risque

- Exécution de code arbitraire à distance
- Déni de service à distance
- Élévation de privilèges

- Atteinte à la confidentialité des données

## Annexe

Bulletins de sécurité Juniper:

- [https://supportportal.juniper.net/s/article/2024-05-Reference-Advisory-Junos-OS-and-Junos-OS-Evolved-Multiple-CVEs-reported-in-OpenSSH?language=en\\_US](https://supportportal.juniper.net/s/article/2024-05-Reference-Advisory-Junos-OS-and-Junos-OS-Evolved-Multiple-CVEs-reported-in-OpenSSH?language=en_US)