Autorité Nationale de Cybersécurité

Djibouti le, 12-07-2024

BULLETIN ALERTES

Object	Multiples Vulnérabilités dans les produits Juniper
Réference	1186
Date de Publication	2024-07-12
Sévérité	Elevé

IMPACT :

- Déni de service
- Exécution de code arbitraire
- Obtention de privilèges
- Perte de confidentialité
- Perte d'intégrité

SYSTÉME AFFECTÉ :

Junos OS Evolved antérieures à :

- 21.2R3-S8-EVO,
- 21.4R3-S6-EVO,
- 21.4R3-S7-EVO,
- 21.4R3-S8-EVO,
- 22.1R3-S5-EVO,
- 22.2R1-EVO,
- 22.2R3- S3-EVO,
- 22.2R3-S4-EVO,
- 22.3R2-S2-EVO,
- 22.3R3-S2-EVO,
- 22.3R3-S3- EVO,
- 22.4R3-EVO,
- 22.4R3-S1-EVO,
- 22.4R3-S3-EVO

Junos OS antérieures à :

- 21.2R3-S8,
- 21.4R3-S5,
- 21.4R3-S8,
- 22.1R3-S4,
- 22.2R3,
- 22.2R3-S4,
- 22.3R2-S2,
- 22.3R3,
- 22.3R3-S3,
- 22.4R2,
- 22.4R3-S3,
- 23.2R1,
- 23.2R2-S1,
- 23.4R1-S2,
- 23.4R2,
- 24.2R1

Junos OS gamme MX Series avec MPC10, MPC11 ou LC9600, MX304 antérieures à :

- 21.2R3-S4,
- 21.4R2,
- 22.2R2-S1,
- 22.2R3,
- 22.3R1

Junos OS Evolved gamme MX Series avec MPC10 MPC11 ou LC9600, MX304 antérieures à :

- 21.2R3-S8-EVO,
- 21.4R2-EVO,
- 22.2R1-EVO

Junos OS Evolved gamme ACX 7000 Series antérieures à :

- 21.4R3-S7- EVO,
- 22.1R3-S6-EVO,
- 22.2R3-S3-EVO,
- 22.3R3-S3-EVO,
- 22.4R3-S2-EVO,
- 23.2R2-EVO,
- 23.4R1-S1-EVO,
- 23.4R2-EVO,
- 24.2R1-EVO

Junos OS gamme RX Series et MX Series avec SPC3 et MS- MPC/MIC antérieures à :

- 20.4R3-S10,
- 21.2R3-S6,
- 21.3R3-S5,
- 21.4R3-S6,
- 22.1R3-S4,
- 22.2R3-S2,
- 22.3R3-S1,
- 22.4R3,
- 23.2R2,
- 23.4R1

Junos OS gamme RX Series, EX Series avec J-Web antérieures à :

- 21.2R3-S8,
- 21.4R3-S7,
- 22.2R3-S4,
- 22.3R3-S3,
- 22.4R3-S2,
- 23.2R2,
- 23.4R1-S1,
- 23.4R2,
- 24.2R1

Junos OS gamme SRX Series, MX Series antérieures à :

- 21.2R3-S6

Junos OS gamme MX240, MX480, MX960 plateformes en utilisant MPC10E antérieures à :

- 20.4R3-S10,

- 21.2R3-S7,
- 21.4R3-S6,
- 22.2R3-S3,
- 22.2R3- S4,
- 22.3R3-S2,
- 22.4R3,
- 23.2R2,
- 23.4R1,
- 23.4R2

Junos OS Evolved gamme PTX Series, ACX Series, QFX Series antérieures à :

- 20.4R3-S7-EVO,
- 21.2R3-S8-EVO,
- 21.4R3-S7-EVO,
- 22.2R3-EVO,
- 22.3R2-EVO,
- 22.4R2-EVO,
- 23.2R1-EVO

Junos OS Evolved antérieures à :

- 23.2R1-S2-EVO,
- 23.2R2-EVO,
- 23.2R2- S1-EVO,
- 23.4R1-EVO,
- 23.4R1-S2-EVO,
- 23.4R2-EVO,
- 24.2R1-EVO

DÉSCRIPTION :

Des nombreuses vulnérabilités ont été découvertes dans les systèmes Juniper Junos OS. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant distant d'exécuter du code arbitraire et de provoquer un déni de service. Parmi elles, la vulnérabilité CVE-2024-39560 est considérée comme la plus élevée. Une description technique détaillée est fournie ci-dessous.

- Nature de la Vulnérabilité

Mauvaise Gestion des Conditions Exceptionnelles : Ce type de vulnérabilité survient lorsque le logiciel ne gère pas correctement les états ou erreurs inattendus.

- Cause

Un voisin RSVP (Resource Reservation Protocol) en aval logiquement adjacent (un autre routeur ou appareil connecté au réseau) peut déclencher cette vulnérabilité. Lorsque ce voisin en aval a une erreur persistante qui reste non corrigée, cela peut entraîner une exhaustion de la mémoire du noyau sur l'appareil Junos OS affecté.

- Vérification

Vous pouvez surveiller l'utilisation de la mémoire du noyau pour détecter des signes de ce problème en utilisant la commande “show system statistics kernel memory”. Voici un exemple de sortie et ce qu'elle indique :

Active: Mémoire actuellement active.

Inactive : Mémoire marquée comme inactive mais pouvant être réactivée.

Wired : Mémoire qui ne peut pas être paginée.

Cached : Mémoire utilisée pour le cache.

Buf : Mémoire utilisée par les tampons.

Free : Mémoire libre disponible.

Kernel Memory (Data/Text) : Utilisation spécifique de la mémoire par le noyau.

Une augmentation inhabituelle de l'utilisation de la mémoire du noyau (Kernel Memory (Data/Text)), en particulier la partie "Data", pourrait indiquer que la vulnérabilité est exploitée, entraînant une exhaustion de la mémoire.

SOLUTION :

Mettre à jour juniper junos os.

DOCUMENTATION :

- Le support Juniper Network :

https://support.juniper.net/support/downloads/

https://supportportal.juniper.net/s/global-search/@uri?language=en_US#sort=relevancy

- CVE-2024-39560

https://www.cve.org/CVERecord?id=CVE-2024-39560

- CVE-2024-39549

https://www.cve.org/CVERecord?id=CVE-2024-39549

- CVE-2024-39530

https://www.cve.org/CVERecord?id=CVE-2024-39530

- CVE-2024-39542

https://www.cve.org/CVERecord?id=CVE-2024-39542

- CVE-2024-39555

https://www.cve.org/CVERecord?id=CVE-2024-39555

- CVE-2024-39531

https://www.cve.org/CVERecord?id=CVE-2024-39531

- CVE-2024-39551

https://www.cve.org/CVERecord?id=CVE-2024-39551

- CVE-2024-39546

https://www.cve.org/CVERecord?id=CVE-2024-39546

- CVE-2024-39553

https://www.cve.org/CVERecord?id=CVE-2024-39553

- CVE-2024-39562

https://www.cve.org/CVERecord?id=CVE-2024-39562

- CVE-2024-39565

https://cve.org/CVERecord?id=CVE-2024-39565

- CVE-2024-39552

https://www.cve.org/CVERecord?id=CVE-2024-39552

- CVE-2024-39518

https://www.cve.org/CVERecord?id=CVE-2024-39518

- CVE-2024-39540

https://www.cve.org/CVERecord?id=CVE-2024-39540

- CVE-2024-39520

https://www.cve.org/CVERecord?id=CVE-2024-39520

- CVE-2024-39521

https://www.cve.org/CVERecord?id=CVE-2024-39521

- CVE-2024-39522

https://www.cve.org/CVERecord?id=CVE-2024-39522

- CVE-2024-39523

https://www.cve.org/CVERecord?id=CVE-2024-39523

- CVE-2024-39524

https://www.cve.org/CVERecord?id=CVE-2024-39524

- CVE-2023-0286

https://www.cve.org/CVERecord?id=CVE-2023-0286

- CVE-2023-0215

https://www.cve.org/CVERecord?id=CVE-2023-0215

- CVE-2022-4450

https://www.cve.org/CVERecord?id=CVE-2022-4450

- CVE-2023-0216

https://www.cve.org/CVERecord?id=CVE-2023-0216

- CVE-2023-0217

https://www.cve.org/CVERecord?id=CVE-2023-0217

- CVE-2023-0401

https://www.cve.org/CVERecord?id=CVE-2023-0401

- CVE-2023-0464

https://www.cve.org/CVERecord?id=CVE-2023-0464

- CVE-2023-5363

https://www.cve.org/CVERecord?id=CVE-2023-5363

- CVE-2023-4807

https://www.cve.org/CVERecord?id=CVE-2023-4807