DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 12-07-2026

BULLETIN ALERTES

Object	Vulnérabilités dans les produits Juniper
Réference	1492
Date de Publication	2026-07-12
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Déni de service à distance
- Divulgation d'informations
- Contournement de mécanismes de sécurité
- Atteinte potentielle à la confidentialité et à l'intégrité des données

SYSTÉME AFFECTÉ :

- Network Director versions antérieures à 7.1R3
- Junos Space versions antérieures à 26.1R1 Patch V1
- Junos OS versions 25.4R1-x antérieures à 25.4R1-S2
- Junos OS versions 25.2R2-x antérieures à 25.2R2-S1
- Junos OS versions 25.2R1-x antérieures à 25.2R1-S2
- Junos OS versions 24.4R2-x antérieures à 24.4R2-S4
- Junos OS versions 24.4R1-x antérieures à 24.4R1-S2
- Junos OS versions 24.2R2-x antérieures à 24.2R2-S5
- Junos OS versions 23.4R2-x antérieures à 23.4R2-S8
- Junos OS versions 23.2R2-x antérieures à 23.2R2-S7
- Junos OS versions 22.4R3-x antérieures à 22.4R3-S10
- Junos OS versions 22.3R3-x antérieures à 22.3R3-S5
- Junos OS versions 22.2R3-x antérieures à 22.2R3-S4
- Junos OS versions 22.1R3-x antérieures à 22.1R3-S6
- Junos OS versions 21.4R3-x antérieures à 21.4R3-S7
- Junos OS versions 21.2R3-x antérieures à 21.2R3-S8
- Junos OS Evolved versions 25.4R1-x antérieures à 25.4R1-S2-EVO
- Junos OS Evolved versions 25.2R2-x antérieures à 25.2R2-S1-EVO
- Junos OS Evolved versions 25.2R1-x antérieures à 25.2R1-S1-EVO
- Junos OS Evolved versions 24.4R2-x antérieures à 24.4R2-S4-EVO
- Junos OS Evolved versions 24.4R1-x antérieures à 24.4R1-S3-EVO
- Junos OS Evolved versions 24.2R2-x antérieures à 24.2R2-S5-EVO
- Junos OS Evolved versions 23.4R2-x antérieures à 23.4R2-S8-EVO
- Junos OS Evolved versions 23.2R2-x antérieures à 23.2R2-S7-EVO
- Junos OS Evolved versions 22.4R3-x antérieures à 22.4R3-S9-EVO
- Junos OS Evolved versions 22.3R3-x antérieures à 22.3R3-S3-EVO
- Junos OS Evolved versions 22.2R3-x antérieures à 22.2R3-S4-EVO
- Junos OS Evolved versions 21.4R3-x antérieures à 21.4R3-S7-EVO
- Junos OS Evolved versions 21.2R3-x antérieures à 21.2R3-S8-EVO
- CTPView versions antérieures à 9.3R2-3
- cRPD versions antérieures à 26.2R1

DÉSCRIPTION :

Plusieurs vulnérabilités ont été corrigées dans les produits **Junos OS**, **Junos OS Evolved**, **Junos Space**, **Network Director**, **CTPView** et **cRPD** de Juniper Networks. Selon la vulnérabilité exploitée, un attaquant pourrait provoquer un déni de service, contourner certains mécanismes de sécurité, divulguer des informations sensibles ou, dans certains cas, exécuter du code arbitraire à distance. Plusieurs vulnérabilités affectent des services réseau essentiels et peuvent entraîner l'interruption de fonctionnalités critiques des équipements concernés.

SOLUTION :

Installer les versions corrigées de Junos OS, Junos OS Evolved, Junos Space, Network Director, CTPView et cRPD conformément aux recommandations de Juniper Networks. Se référer aux bulletins de sécurité publiés le **8 juillet 2026** pour connaître les versions corrigées applicables à chaque produit et les éventuelles mesures d'atténuation.

DOCUMENTATION :

Bulletins de sécurité Juniper

- https://supportportal.juniper.net/s/article/2026-07-Security-Bulletin-CTPView-Multiple-vulnerabilities-resolved-in-9-3R2-3-Release
- https://supportportal.juniper.net/s/article/2026-07-Security-Bulletin-Junos-OS-Evolved-URL-handling-vulnerability-in-libfetch-results-in-heap-buffer-overflow-CVE-2020-7450
- https://supportportal.juniper.net/s/article/2026-07-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-26-1R1-Patch-V1-Release
- https://supportportal.juniper.net/s/article/2026-07-Security-Bulletin-Network-Director-Multiple-vulnerabilities-resolved-in-7-1R3-release
- https://supportportal.juniper.net/s/article/2026-07-Security-Bulletin-cRPD-Multiple-vulnerabilities-resolved-in-cRPD-26-2R1

CVE-2020-7450 :

- https://www.cve.org/CVERecord?id=CVE-2020-7450

CVE-2026-21901 :

- https://www.cve.org/CVERecord?id=CVE-2026-21901

CVE-2026-33794 :

- https://www.cve.org/CVERecord?id=CVE-2026-33794

CVE-2026-33799 :

- https://www.cve.org/CVERecord?id=CVE-2026-33799

CVE-2026-33800 :

- https://www.cve.org/CVERecord?id=CVE-2026-33800

CVE-2026-33801 :

- https://www.cve.org/CVERecord?id=CVE-2026-33801

CVE-2026-33802 :

- https://www.cve.org/CVERecord?id=CVE-2026-33802

CVE-2026-33803 :

- https://www.cve.org/CVERecord?id=CVE-2026-33803

CVE-2026-57019 :

- https://www.cve.org/CVERecord?id=CVE-2026-57019

CVE-2026-57020 :

- https://www.cve.org/CVERecord?id=CVE-2026-57020

CVE-2026-57021 :

- https://www.cve.org/CVERecord?id=CVE-2026-57021

CVE-2026-57022 :

- https://www.cve.org/CVERecord?id=CVE-2026-57022

CVE-2026-57023 :

- https://www.cve.org/CVERecord?id=CVE-2026-57023

CVE-2026-57024 :

- https://www.cve.org/CVERecord?id=CVE-2026-57024

CVE-2026-57025 :

- https://www.cve.org/CVERecord?id=CVE-2026-57025

CVE-2026-57026 :

- https://www.cve.org/CVERecord?id=CVE-2026-57026

CVE-2026-57027 :

- https://www.cve.org/CVERecord?id=CVE-2026-57027

CVE-2026-57028 :

- https://www.cve.org/CVERecord?id=CVE-2026-57028

CVE-2026-57029 :

- https://www.cve.org/CVERecord?id=CVE-2026-57029

CVE-2026-57030 :

- https://www.cve.org/CVERecord?id=CVE-2026-57030

CVE-2026-57031 :

- https://www.cve.org/CVERecord?id=CVE-2026-57031

CVE-2026-57032 :

- https://www.cve.org/CVERecord?id=CVE-2026-57032

CVE-2026-57054 :

- https://www.cve.org/CVERecord?id=CVE-2026-57054