ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilité dans les produits Juniper
Numéro de Référence	52731402/25
Date de Publication	14 Février 2025
Risque	Important
Impact	Important

Systèmes affectés

- WAN Assurance Managed Routers versions 6.x antérieures à 6.1.12-lts
- WAN Assurance Managed Routers versions 6.3.x antérieures à 6.3.3-r2
- WAN Assurance Managed Routers versions 6.2.x antérieures à 6.2.8-lts
- WAN Assurance Managed Routers versions 5.6.x antérieures à 5.6.17
- Session Smart Router versions 6.x antérieures à 6.1.12-lts
- Session Smart Router versions 6.3.x antérieures à 6.3.3-r2
- Session Smart Router versions 6.2.x antérieures à 6.2.8-lts
- Session Smart Router versions 5.6.x antérieures à 5.6.17
- Session Smart Conductor versions 6.x antérieures à 6.1.12-lts
- Session Smart Conductor versions 6.3.x antérieures à 6.3.3-r2
- Session Smart Conductor versions 6.2.x antérieures à 6.2.8-lts
- Session Smart Conductor versions 5.6.x antérieures à 5.6.17

Identificateurs externes

- CVE-2025-21589

Bilan de la vulnérabilité

Juniper annonce la correction d'une vulnérabilité dans les versions susmentionnées des produits Juniper Networks. L'exploitation de cette faille peut permettre à un attaquant de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité Juniper du 11 Février 2025 pour plus d'information.

Risque

- Contournement de la politique de sécurité

Annexe

Bulletin de sécurité Juniper du 11 Février 2025:

- https://supportportal.juniper.net/s/article/2025-02-Out-of-Cycle-Security-Bulletin-Session-Smart-Router-Session-Smart-Conductor-WAN-Assurance-Router-API-Authentication-Bypass-Vulnerability-CVE-2025-21589?language=en_US