ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités activement exploitées affectant Juniper Secure Analytics
Numéro de Référence	61101302/26
Date de Publication	13 février 2026
Risque	Important
Impact	Critique

Systèmes affectés

- Juniper Secure Analytics (JSA) versions 7.5.0 antérieures à 7.5.0 UP14 IF01

Identificateurs externes

CVE-2020-16971 CVE-2022-49985 CVE-2022-50087 CVE-2023-53125 CVE-2023-53373
CVE-2024-47252 CVE-2024-47619 CVE-2025-22026 CVE-2025-23048 CVE-2025-32988
CVE-2025-32990 CVE-2025-37797 CVE-2025-38350 CVE-2025-38352 CVE-2025-38392
CVE-2025-38449 CVE-2025-38461 CVE-2025-38498 CVE-2025-38527 CVE-2025-38556
CVE-2025-38718 CVE-2025-39730 CVE-2025-39757 CVE-2025-40928 CVE-2025-41244
CVE-2025-49630 CVE-2025-49812 CVE-2025-5318 CVE-2025-55752 CVE-2025-61795
CVE-2025-6395

Bilan de la vulnérabilité

Juniper annonce la correction de plusieurs vulnérabilités affectant les versions susmentionnées de son produit « Juniper Secure Analytics ». Certaines de ces vulnérabilités sont susceptibles d'être activement exploitées. Un attaquant pourrait profiter de ces vulnérabilités pour exécuter du code à distance, accéder à des données confidentielles, élever ses privilèges, contourner des mesures de sécurité ou causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de Juniper afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire
- Accès à des données confidentielles
- Elévation de privilèges
- Contournement de mesures de sécurité
- Déni de service

Référence

Bulletin de sécurité Juniper:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP14-IF01