SAP Security Note

3695912 - [CVE-2026-24324] Vulnérabilité de déni de service (DOS) dans la plateforme SAP BusinessObjects Business Intelligence (AdminTools)

Composant: BI-BIP-SRV (Solutions de Business Intelligence > Plateforme de Business Intelligence > Problèmes de CMS/d'audit (à l'exclusion de l'authentification tierce)), Version: 5, Validé le: 24.02.2026

⚠ Attention. Ceci est un outil de traduction automatisé dont la mise au point n'est pas finalisée.

Symptôme

La plateforme SAP BusinessObjects Business Intelligence (AdminTools) permet à un attaquant authentifié disposant de privilèges utilisateur d'exécuter une requête spécifique dans AdminTools qui pourrait entraîner une panne du serveur de gestion du contenu (CMS), rendant le CMS partiellement ou complètement indisponible et entraînant le refus de service du Content Management Server (CMS). Une exploitation réussie a un impact sur la disponibilité du système, tandis que la confidentialité et l'intégrité ne sont pas affectées.

Journal des modifications :

v5 (version actuelle) - **MISE À JOUR du 24 février 2026** : cette note a été republiée avec la section « Solution » mise à jour.

v4 (Version initiale validée pour les clients)

Autres termes

Denial of Service (DoS), Resource Exhaustion, Uncontrolled Resource Consumption, CVE-2026-24324

Motif et conditions préalables

Le serveur a exécuté des fonctions non valides dans la requête.

Solution

Par cette correction, le filtrage et les restrictions requis sont implémentés.

Implémentez les Support Packages et correctifs référencés dans cette note de sécurité SAP.

Pour connaître la stratégie et le calendrier de maintenance de la plateforme de Business Intelligence, reportez-vous à l'article de la base de connaissances 2144559 dans la section Références.

CVSS

Note CVSS : 6.5

Vecteur CVSS : CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Vecteur d'attaque (AV)	Réseau (N)
Complexité d'attaque (AC)	Faible (L)
Privilèges requis (PR)	Faible (L)
Interaction utilisateur (IU)	Aucun (N)
Périmètre (S)	Non modifié (U)
Impact de confidentialité (C)	Aucun (N)
Impact sur l'intégrité (I)	Aucun (N)
Impact de disponibilité (A)	Élevé (H)

SAP provides this CVSS v3.0 base score as an estimate of the risk posed by the issue reported in this note. This estimate does not take into account your own system configuration or operational environment. It is not intended to replace any risk assessments you are advised to conduct when deciding on the applicability or priority of this SAP security note. For more information, see the FAQ section at https://support.sap.com/securitynotes .

Attributs

Clé	Val.
Signalé en externe	Oui

Composantes logicielles

Composante logicielle	De	Au
ENTERPRISE	430	430
ENTERPRISE	2025	2025
ENTERPRISE	2027	2027

Correctifs de Support Package

Version de composante logicielle	Support Packages	Numéro de Support Package	
SBOP BI PLATFORM SERVERS 2027	SP000	000000	
SBOP BI PLATFORM SERVERS 4.3	SP004	001700	
SBOP BI PLATFORM SERVERS 4.3	SP005	000400	
SBOP BI PLATFORM SERVERS 2025	SP000	000800	