SAP Security Note

3696239 - [CVE-2025-64775] Vulnérabilité au déni de service dans la plateforme SAP BusinessObjects Business Intelligence

Composant: BI-BIP-SEC (Solutions de Business Intelligence > Plateforme de Business Intelligence > Vulnérabilités de sécurité dans SAP BusinessObjects), Version: 10, Validé le: 14.04.2026

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

Symptôme

La plateforme SAP BusinessObjects Business Intelligence, à l'aide d'Apache Struts, permet à un attaquant d'épuiser les ressources du système par le biais d'une fuite de fichiers dans le traitement des demandes en plusieurs parties, provoquant des pannes de service ou des inondations qui entraînent un déni de service. Cela entraîne un fort impact sur la disponibilité, sans impact sur la confidentialité et l'intégrité de l'application.

Autres termes

DoS, DDoS, Déni de service distribué, Consommation incontrôlée des ressources, Épuisement des ressources, CVE-2025-64775

Motif et conditions préalables

Nettoyage incomplet des ressources temporaires lors du traitement des requêtes en plusieurs parties dans Apache Struts (de 2.0.0 à la version 6.7.0).

Solution

Le problème a été résolu par la mise à niveau de la bibliothèque Apache Struts intégrée à la version 6.8.0 ou 7.1.1, garantissant une gestion correcte des ressources et empêchant la consommation de ressources non contrôlées.

Implémentez les correctifs répertoriés dans la section "Support Packages & Patches" de cette note de sécurité SAP.

Pour le calendrier et la stratégie de maintenance de la plateforme de Business Intelligence, voir 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	000900	