



3654236 - [CVE-2026-0490] Dénî de service (DOS) dans la plateforme SAP BusinessObjects BI

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: 6, Validé le: 10.02.2026

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

Symptôme

La plateforme SAP BusinessObjects BI permet à un attaquant non authentifié de créer une requête réseau spécifique vers le point de terminaison de confiance qui interrompt l'authentification, ce qui empêche les utilisateurs légitimes d'accéder à la plateforme. Par conséquent, elle a un impact élevé sur la disponibilité, mais n'a aucun impact sur la confidentialité et l'intégrité.

Autres termes

DoS, DDoS, Dénî de service distribué, Connexion, [CVE-2026-0490](#)

Motif et conditions préalables

Les serveurs d'applications Web n'ont pas vérifié si la demande spécifique provenait d'un système légitime.

Solution

Avec ce correctif, les clients sont désormais autorisés à configurer le point de terminaison de confiance de l'application Web avec TLS mutuel (mTLS) pour accepter uniquement les requêtes des serveurs backend approuvés.

Implémentez les Support Packages et correctifs référencés dans cette note de sécurité SAP. Après l'installation du correctif, suivez l'[l'article 3672038 de la base de connaissances](#) pour configurer l'authentification basée sur un certificat.

Pour connaître la planification et la stratégie de maintenance de la plateforme de Business Intelligence, voir l'[l'article de la base de connaissances 2144559](#) dans la section Références.

Solution de contournement

Évaluez l'applicabilité de la solution de contournement pour votre infrastructure SAP avant l'implémentation. Notez que cette solution de contournement est un correctif temporaire et n'est pas une solution permanente. SAP vous recommande vivement d'appliquer les corrections décrites dans la note de sécurité, qui peuvent être effectuées à la place de la solution de contournement ou après l'implémentation de la solution de contournement.

- L'infrastructure doit être séparée en un réseau interne pour la communication des services de niveau Web et backend, et en un réseau externe pour l'accès de l'utilisateur au niveau Web. Les demandes du réseau externe vers l'URL autorisée doivent être bloquées.

| CVSS

Note CVSS : 7.5

Vecteur CVSS : CVSS:3.0/AV:N/AC:L/PR:N/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)	Aucun (N)
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.
Autres composants	Solutions de Business Intelligence > Plateforme de Business Intelligence > Central Management Console (CMC) (BI-BIP-CMC)
Autres composants	Solutions de Business Intelligence > Plateforme de Business Intelligence > InfoView, zone de lancement BI (BI-BIP-INV)
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	001600	
SBOP BI PLATFORM SERVERS 4.3	SP005	000400	
SBOP BI PLATFORM SERVERS 2025	SP000	000700	

| Ce document fait référence à

Note SAP/Article de la base de connaissances	Composant	Titre
3672038	BI-BIP-AUT	<u>Implémentation de l'authentification par certificat client pour le point de terminaison du jeton de confiance</u>
2144559	BI-BIP	<u>Planification et stratégie de maintenance de la plateforme SAP BusinessObjects BI</u>