



3674246 - [CVE-2026-0508] Ouvrir la vulnérabilité de redirection 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: 7, 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 Business Intelligence permet à un attaquant authentifié disposant de droits élevés d'insérer une URL malveillante dans l'application. Une fois l'exploitation réussie, la victime peut cliquer sur cette URL malveillante, ce qui se traduit par une redirection non validée vers le domaine contrôlé par l'attaquant et par la suite télécharger le contenu malveillant. Cette vulnérabilité a un impact élevé sur la confidentialité et l'intégrité de l'application, sans effet sur la disponibilité de l'application.

Autres termes

Ouvrir la redirection, validation manquante, [CVE-2026-0508](#)

Motif et conditions préalables

La vulnérabilité est survenue en raison de l'application permettant le partage des liens sans effectuer la validation nécessaire.

Solution

Par cette correction, la liste blanche côté serveur a été implémentée pour empêcher toute redirection non validée vers des URL tierces.

Implémentez les Support Packages référencés par cette note de sécurité SAP.

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

Solution de contournement :

Aucune solution de contournement n'est disponible pour cette note de sécurité.

| CVSS

Note CVSS : 7.3

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

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

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	001600	
SBOP BI PLATFORM SERVERS 4.3	SP005	000400	
SBOP BI PLATFORM SERVERS 2025	SP000	000800	

Ce document fait référence à

Note SAP/Article de la base de connaissances	Composant	Titre
2144559	BI-BIP	<u>Planification et stratégie de maintenance de la plateforme SAP BusinessObjects BI</u>