



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits SAP
Numéro de Référence	59040912/25
Date de publication	09 décembre 2025
Risque	Important
Impact	Critique

Systemes affectés

- SAP Solution Manager Version(s) - ST 720
- SAP Commerce Cloud Version(s) - HY_COM 2205, COM_CLOUD 2211, COM_CLOUD 2211-JDK21
- SAP jConnect - SDK for ASE Version(s) - SYBASE_SOFTWARE_DEVELOPER_KIT 16.0.4, 16.1
- SAP Web Dispatcher and Internet Communication Manager (ICM) Version(s) - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, WEBDISP 7.22_EXT, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.16
- SAP NetWeaver (remote service for Xcelsius) Version(s) - BI-BASE-E 7.50, BI-BASE-B 7.50, BI-IBC 7.50, BI-BASE-S 7.50, BIWEBAPP 7.50
- SAP Business Objects Version(s) – ENTERPRISE 430, 2025, 2027
- SAP Web Dispatcher, Internet Communication Manager and SAP Content Server Version(s) - KRNL64UC 7.53, WEBDISP 7.53, 7.54, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1, CONTSERV 7.53, 7.54, KERNEL 7.53, 7.54
- SAP S/4 HANA Private Cloud (Financials General Ledger) Version(s) - S4CORE 104, 105, 106, 107, 108, 109
- SAP NetWeaver Internet Communication Framework Version(s) - SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758
- Application Server ABAP Version(s) - KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.16, 9.17
- SAP NetWeaver Enterprise Portal Version(s) - EP-RUNTIME 7.50

- SAPUI5 framework (Markdown-it component) Version(s) - SAP_UI 755, 756, 757, 758
- SAP Enterprise Search for ABAP Version(s) - SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816
- SAP BusinessObjects Business Intelligence Platform Version(s) - ENTERPRISE 430, 2025, 2027

Identificateurs externes

CVE-2025-42872	CVE-2025-42873	CVE-2025-42874	CVE-2025-42875	CVE-2025-42876
CVE-2025-42877	CVE-2025-42878	CVE-2025-42880	CVE-2025-42891	CVE-2025-42896
CVE-2025-42904	CVE-2025-42928	CVE-2025-48976	CVE-2025-55752	CVE-2025-55754

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du code, de contourner des mesures de sécurité ou d'accéder à des données confidentielles ou de causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité de SAP afin d'installer les nouvelles mises à jour.

Risque

- Injection de code
- Contournement de mesures de sécurité
- Accès à des données confidentielles
- Déni de service

Référence

Bulletin de sécurité de SAP:

- <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2025.html>