



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits SAP
Numéro de Référence	54991106/25
Date de publication	11 Juin 2025
Risque	Critique
Impact	Critique

Systemes affectés

- SAP NetWeaver Application Server for ABAP Versions – KERNEL 7.89, 7.93, 9.14, 9.15
- SAP GRC (AC Plugin) Versions – GRCPINW V1100_700, V1100_731
- SAP Business Warehouse and SAP Plug-In Basis Versions – PI_BASIS 2006_1_700, 701, 702, 731, 740, SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, 758, 914, 915
- SAP BusinessObjects Business Intelligence (BI Workspace) Versions – ENTERPRISE 430, 2025, 2027
- SAP NetWeaver Visual Composer Version – VCBASE 7.50
- SAP MDM Server Versions – MDM_SERVER 710.750
- SAP S/4HANA (Enterprise Event Enablement) Versions – SAP_GWFND 757, 758
- SAP NetWeaver (ABAP Keyword Documentation) Version – SAP_BASIS 758
- SAP S/4HANA (Manage Central Purchase Contract application) Versions – S4CORE 106, 107, 108
- SAP Business One Integration Framework Versions – B1_ON_HANA 10.0, SAP-M-BO 10.0
- SAP S/4HANA (Manage Processing Rules - For Bank Statement) Versions – S4CORE 104, 105, 106, 107, 108
- SAP S/4HANA (Bank Account Application) Version – S4CORE 108
- SAP Business Objects Business Intelligence Platform Versions - ENTERPRISE 430, 2025, 2027
- SAPUI5 applications Versions – SAP_UI 750, 754, 755, 756, 757, 758, UI_700 200

Identificateurs externes

CVE-2025-23192	CVE-2025-31325	CVE-2025-42977	CVE-2025-42982	CVE-2025-42983
CVE-2025-42984	CVE-2025-42987	CVE-2025-42988	CVE-2025-42989	CVE-2025-42990
CVE-2025-42991	CVE-2025-42993	CVE-2025-42994	CVE-2025-42995	CVE-2025-42996
CVE-2025-42998				

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 contenu dans une page, de contourner des mesures de sécurité ou d'accéder à des données confidentielles.

Solution

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

Risque

- Injection de de contenu dans une page
- Contournement de mesures de sécurité
- Accès à des données confidentielles

Référence

Bulletin de sécurité de SAP:

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