



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits SAP
Numéro de Référence	54431405/25
Date de publication	14 Mai 2025
Risque	Critique
Impact	Critique

Systemes affectés

- SAP NetWeaver (Visual Composer development server) Version – VCFRAMEWORK 7.50
- SAP Supplier Relationship Management (Live Auction Cockpit) Version – SRM_SERVER 7.14
- SAP S/4HANA Cloud Private Edition or on Premise (SCM Master Data Layer (MDL)) Versions – S4CORE 102, 103, 104, 105, 106, 107, 108, SCM_BASIS 700, 701, 702, 712, 713, 714
- SAP Business Objects Business Intelligence Platform (PMW) Versions – ENTERPRISE 430, 2025, 2027
- SAP Landscape Transformation (PCL Basis) Versions – DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752, 2020, S4CORE 102, 103, 104, 105, 106, 107, 108
- SAP PDCE Versions – S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108
- SAP Gateway Client Versions – SAP_GWFND 752, 753, 754, 755, 756, 757, 758
- SAP S/4HANA (Private Cloud & On-Premise) Versions - S4CRM 204, 205, 206, S4CEXT 107, 108, BBPCRM 702, 712, 713, 714
- SAP Service Parts Management (SPM) Versions - SAP_APPL 600, 602, 603, 604, 605, 606, 616, 617, 618, SAPSCORE 111, S4CORE 100, 101, 102
- SAP Service Parts Management (SPM) Versions - SAP_APPL 617, 618, SAPSCORE 116, S4CORE 100, 101, 102, 103
- SAP NetWeaver Application Server ABAP and ABAP Platform Versions - 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
- SAP Supplier Relationship Management (Master Data Management Catalog) Version –

SRM_MDM_CAT 7.52

- SAP S/4HANA HCM Portugal and SAP ERP HCM Portugal Versions – S4HCMCPT 100, 101, SAP_HRCPT 600, 604, 608
- SAP Digital Manufacturing (Production Operator Dashboard) Version – CTNR-DME-PODFoundation-MS 1.0
- SAP Data Services Management Console Version – SBOP DS JOB SERVER 4.3
- SAP S/4HANA (OData meta-data property) Versions - S4CORE 102, 103, 104, 105, 106
- SAP GUI for Windows Version – BC-FES-GUI 8.00

Identificateurs externes

CVE-2024-39592	CVE-2025-26662	CVE-2025-30009	CVE-2025-30010	CVE-2025-30011
CVE-2025-30012	CVE-2025-30018	CVE-2025-31324	CVE-2025-31329	CVE-2025-42997
CVE-2025-42999	CVE-2025-43000	CVE-2025-43002	CVE-2025-43003	CVE-2025-43004
CVE-2025-43005	CVE-2025-43006	CVE-2025-43007	CVE-2025-43008	CVE-2025-43009
CVE-2025-43010	CVE-2025-43011			

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/may-2025.html>