ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant plusieurs produits SAP
Numéro de Référence	53131103/25
Date de publication	11 Mars 2025
Risque	Important
Impact	Important

Systèmes affectés

- SAP Commerce (Swagger UI), Version – COM_CLOUD 2211
- SAP NetWeaver (ABAP Class Builder), 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_BASIS 914
- SAP Commerce Cloud, Version -HY-COM 2205, COM-CLOUD 2211
- sap/approuter, Version - 2.6.1 to 16.7.1
- SAP PDCE, Version – S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108
- SAP Business One (Service Layer), Version - B1_ON_HANA 10.0, SAP-M-BO 10.0
- SAP NetWeaver Application Server ABAP (applications based on SAP GUI for HTML), Versions – KRNL64UC 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.89, KERNEL 7.93, KERNEL 9.14
- SAP NetWeaver Application Server ABAP, Version – 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_BASIS 914
- SAP Business Warehouse (Process Chains), Version – DW4CORE 100, DW4CORE 200, DW4CORE 300, DW4CORE 400, DW4CORE 914, SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 750
- SAP NetWeaver Application Server Java, Version – AJAX-RUNTIME 7.50
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence), Version – ENTERPRISE 430, 2025
- SAP NetWeaver Enterprise Portal (OBN component), Version – EP-RUNTIME 7.50
- SAP Web Dispatcher and Internet Communication Manager, Versions – KRNL64UC 7.53,

WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.89, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.89, KERNEL 7.93, KERNEL 9.14

- SAP BusinessObjects Business Intelligence Platform, Version – ENTERPRISE 430, 2025, ENTERPRISECLIENTTOOLS 430, 2025
- SAP S/4HANA (Manage Bank Statements), Versions – S4CORE 107, S4CORE 108
- SAP S/4HANA (RBD), Versions – S4CORE 102, 103, 104, 105, 106, 107, 108, EA-FINSERV 618, EA-FINSERV 800
- SAP Fiori apps (Posting Library), Version – S4CORE 103, 104, 105, 106, 107, 108
- SAP Just In Time, Version - S4CORE 105, 106, 107, 108
- SAP Permit to Work, Versions - UIS4HOP1 800, 900
- SAP Business Objects Business Intelligence Platform, Version - ENTERPRISE 430, 2025, 2027
- SAP Commerce Cloud and SAP Datahub, , Version -HY_COM 2205, HY_DHUB 2205, COM_CLOUD 2211, DHUB_CLOUD 2211
- SAP CRM and SAP S/4HANA (Interaction Center), Versions - S4CRM 100, 200, 204, 205, 206, S4FND 102, 103, 104, 105, 106, 107, 108, S4CEXT 107, 108, BBPCRM 701, 702, 712, 713, 714, WEBCUIF 701, 731, 746, 747, 748, 800, 801
- SAP Just In Time, Version - S4CORE 102, 103, 104, 105, 106, 107, ECC-DIMP 618
- SAP Electronic Invoicing for Brazil (eDocument Cockpit), Version - SAP_APPL 617, 618, S4CORE 102, 103, 104, 105, 106, 107, 108

Identificateurs externes

CVE-2024-38286	CVE-2024-38819	CVE-2024-38820	CVE-2024-39592	CVE-2024-41736
CVE-2024-52316	CVE-2025-0062	CVE-2025-0071	CVE-2025-23185	CVE-2025-23188
CVE-2025-23194	CVE-2025-24876	CVE-2025-25242	CVE-2025-25244	CVE-2025-25245
CVE-2025-26655	CVE-2025-26656	CVE-2025-26658	CVE-2025-26659	CVE-2025-26660
CVE-2025-26661	CVE-2025-27430	CVE-2025-27431	CVE-2025-27432	CVE-2025-27433
CVE-2025-27434	CVE-2025-27436			

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 un site, 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/march-2025.html