ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits SAP
Numéro de Référence	56620909/25
Date de Publication	09 Septembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Supplier Relationship Management versions RM_SERVER 700, 701, 702, 713 et 714
- S/4HANA (Private Cloud or On-Premise) versions S4CORE 102, 103, 104, 105, 106, 107 et 108
- Netweaver (RMI-P4) version SERVERCORE 7.50
- NetWeaver versions KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53 et 7.54
- NetWeaver and ABAP Platform (Service Data Collection) versions ST-PI 2008_1_700, 2008_1_710 et 740
- NetWeaver Application Server for ABAP 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 et SAP_BASIS 816
- NetWeaver Application Server for ABAP (Background Processing) 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 et SAP_BASIS 816

- NetWeaver Application Server Java version WD-RUNTIME 7.50
- NetWeaver AS for ABAP and ABAP Platform versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756 et 757
- NetWeaver AS Java (IIOP Service) version SERVERCORE 7.50
- NetWeaver AS Java (Deploy Web Service) version J2EE-APPS 7.50
- NetWeaver AS Java (Adobe Document Service) version ADSSAP 7.50
- NetWeaver ABAP Platform versions S4CRM 100, 200, 204, 205, 206, S4CEXT 109, BBPCRM 713 et 714
- NetWeaver (Service Data Download) 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 et SAP_BASIS 816
- Landscape Transformation Replication Server versions DMIS 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752 et 2020
- HCM (My Timesheet Fiori 2.0 application) version GBX01HR5 605
- HCM (Approve Timesheets Fiori 2.0 application) version GBX01HR5 605
- Fiori app (Manage Payment Blocks) versions S4CORE 107 et 108
- Fiori App (F4044 Manage Work Center Groups) versions UIS4HOP1 600, 700, 800 et 900
- Fiori (Launchpad) version SAP_UI 754
- Commerce Cloud versions HY_COM 2205 et COM_CLOUD 2211
- Commerce Cloud and Datahub versions HY_COM 2205, HY_DHUB 2205, COM_CLOUD 2211 et DHUB_CLOUD 2211
- BusinessObjects Business Intelligence Platform versions ENTERPRISE 430, 2025 et 2027

- Business Planning and Consolidation versions BPC4HANA 200, 300, SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, 758, 816, 914 et CPMBPC 810
- Business One (SLD) versions B1_ON_HANA 10.0 et SAP-M-BO 10.0

Identificateurs externes

- CVE-2023-27500 CVE-2023-5072 CVE-2024-13009
- CVE-2025-22228 CVE-2025-27428 CVE-2025-42911
- CVE-2025-42912 CVE-2025-42913 CVE-2025-42914
- CVE-2025-42915 CVE-2025-42916 CVE-2025-42917
- CVE-2025-42918 CVE-2025-42920 CVE-2025-42922
- CVE-2025-42923 CVE-2025-42925 CVE-2025-42926
- CVE-2025-42927 CVE-2025-42929 CVE-2025-42930
- CVE-2025-42933 CVE-2025-42938 CVE-2025-42941
- CVE-2025-42944 CVE-2025-42958 CVE-2025-42961

Bilan de la vulnérabilité

SAP a publié des correctifs de sécurité, dont trois vulnérabilités critiques affectant la plateforme SAP NetWeaver, largement utilisée dans les environnements d'entreprise. La faille la plus grave (CVE-2025-42944, score CVSS 10.0) concerne une vulnérabilité de désérialisation non sécurisée dans NetWeaver ServerCore 7.50 (RMI-P4). Exploitée via un port RMI-P4 ouvert, elle permet à un attaquant non authentifié d'exécuter des commandes arbitraires sur le système. Les deux autres vulnérabilités critiques incluent CVE-2025-42922 (CVSS 9.9), qui permet le téléchargement de fichiers arbitraires via la fonctionnalité de déploiement de services web, et CVE-2025-42958 (CVSS 9.1), un défaut d'authentification autorisant des utilisateurs non autorisés à accéder à des fonctions administratives sensibles et à manipuler des données critiques.

En complément, SAP a corrigé plusieurs failles permettant à un attaquant de porter atteinte à la confidentialité et l'intégrité des données, de contourner la politique de sécurité, voire, dans certaines conditions, de prendre le contrôle total du système.

Solution

Veuillez se référer au bulletin de sécurité de SAP du 09 Septembre 2025 afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données
- Contournement de la politique de sécurité
- Prise de contrôle du système

Référence

Bulletin de sécurité SAP du 09 Septembre 2025:

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

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma