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	53760804/25
Date de Publication	08 Avril 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP BusinessObjects Business Intelligence Platform – ENTERPRISE 430
- SAP BusinessObjects Business Intelligence platform (Central Management Console) – ENTERPRISE 430, 2025
- SAP CRM and SAP S/4HANA (Interaction Center) – 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 Capital Yield Tax Management – CYTERP 420_700, CYT 800, IBS 7.0, CYT4HANA 100
- SAP Commerce Cloud (Public Cloud) – COM_CLOUD 2211
- SAP Commerce Cloud – HY_COM 2205, COM_CLOUD 2211
- SAP ERP BW Business Content – BI_CONT 707, 737, 747, 757
- SAP Financial Consolidation – FINANCE 1010
- SAP KMC WPC – KMC-WPC 7.50
- SAP Landscape Transformation (Analysis Platform) – DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731
- SAP NetWeaver AS ABAP (SAP GUI for HTML) – KRNL64NUC 7.22, 7.22EXT ; KRNL64UC 7.22, 7.22EXT ; 7.53, 7.54, 7.77, 7.89, 7.93, 9.14
- SAP NetWeaver AS ABAP (Virus Scan Interface) – SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758
- SAP NetWeaver Application Server ABAP – KRNL64NUC 7.22, 7.22EXT ; KRNL64UC 7.22, 7.22EXT ; 7.53, 7.54, 7.77, 7.89, 7.93
- SAP NetWeaver and ABAP Platform (AS ABAP) – KRNL64UC 7.53, KERNEL 7.53, 7.54

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- SAP NetWeaver and ABAP Platform (Service Data Collection) – ST-PI 2008_1_700, 2008_1_710, 740
- SAP NetWeaver – SAP_ABA 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, 75I
- SAP S/4HANA (Private Cloud) – S4CORE 102, 103, 104, 105, 106, 107, 108
- SAP S4CORE entity – S4CORE 107, 108
- SAP Solution Manager – ST 720, SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 914

Identificateurs externes

- CVE-2024-56337 CVE-2025-0064 CVE-2025-23186
- CVE-2025-26653 CVE-2025-26654 CVE-2025-26657
- CVE-2025-27428 CVE-2025-27429 CVE-2025-27430
- CVE-2025-27435 CVE-2025-27437 CVE-2025-30013
- CVE-2025-30014 CVE-2025-30015 CVE-2025-30016
- CVE-2025-30017 CVE-2025-31330 CVE-2025-31331
- CVE-2025-31332 CVE-2025-31333

Bilan de la vulnérabilité

SAP annonce la disponibilité d'une mise à jour de sécurité corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire, de porter atteinte à la confidentialité de données et de contourner la politique de sécurité.

Solution

Veuillez se référer au bulletin de sécurité SAP du 08 Avril 2025**.**

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Exécution du code arbitraire

Annexe

Bulletin de sécurité SAP du 08 Avril 2025**:**

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