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	55560807/25
Date de Publication	08 Juillet 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP Business Warehouse & SAP Plug-In Basis PI_BASIS 2006_1_700, 701, 702, 731, 740 ; SAP_BW 700–758, 816 ; SAP_BW_VIRTUAL_COMP 701
- SAP BusinessObjects Business Intelligence Platform (CMC, Web Intelligence) ENTERPRISE 430, 2025, 2027 ; ENTERPRISECLIENTTOOLS 430, 2025, 2027
- SAP Data Services (DQ Report) SBOP_DS_MANAGEMENT_CONSOLE 4.3, 2025
- SAP GUI pour Windows BC-FES-GUI 8.00
- SAP NetWeaver & ABAP Platform (SDCCN) ST-PI 2008_1_700, 2008_1_710, 740
- SAP NetWeaver (RFC enabled function module) SAP_BW 700–758, 816, 914, 916
- SAP NetWeaver (XML Data Archiving Service) J2EE-APPS 7.50
- SAP NetWeaver ABAP Server / ABAP Platform SAP_BASIS 700–758, 914, 915, 816
- SAP NetWeaver AS Java (TLS hostname validation) ENGINEAPI 7.50
- SAP NetWeaver Application Server pour Java (Log Viewer) LMNWABASICAPPS 7.50
- SAP NetWeaver Enterprise Portal (Federated Portal Network & Administration) EP-RUNTIME 7.50
- SAP NetWeaver Visual Composer VCBASE 7.50

- SAP S/4HANA & SAP SCM (Characteristic Propagation) SCMAPO 713, 714 ; S4CORE 102, 103, 104 ; S4COREOP 105, 106, 107, 108 ; SCM 700, 701, 702, 712
- SAP S/4HANA (Enterprise Event Enablement) SAP_GWFND 757, 758
- SAP Supplier Relationship Management (Live Auction Cockpit) SRM_SERVER 7.14
- SAPCAR SAP_CAR 7.53, 7.22EXT

Identificateurs externes

- CVE-2024-53677 CVE-2025-30009 CVE-2025-30010
- CVE-2025-30011 CVE-2025-30012 CVE-2025-30018
- CVE-2025-31326 CVE-2025-42952 CVE-2025-42953
- CVE-2025-42954 CVE-2025-42959 CVE-2025-42960
- CVE-2025-42961 CVE-2025-42962 CVE-2025-42963
- CVE-2025-42964 CVE-2025-42965 CVE-2025-42966
- CVE-2025-42967 CVE-2025-42968 CVE-2025-42969
- CVE-2025-42970 CVE-2025-42971 CVE-2025-42973
- CVE-2025-42974 CVE-2025-42977 CVE-2025-42978
- CVE-2025-42979 CVE-2025-42980 CVE-2025-42981
- CVE-2025-42985 CVE-2025-42986 CVE-2025-42993
- CVE-2025-43001

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les produits SAP. L'exploitation de ces failles permet à un attaquant distant de causer un déni de service, de réussir une élévation de privilèges, 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 08 Juillet 2025 afin d'installer les nouvelles mises à jour.

Risque

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

Référence

Bulletin de sécurité SAP du 08 Juillet 2025:

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