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	63091404/26
Date de Publication	14 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP Business Planning and Consolidation et SAP Business Warehouse versions HANABPC 810, BPC4HANA 300, SAP_BW 750, 752, 753, 754, 755, 756, 757, 758, 816
- SAP ERP et SAP S/4 HANA versions SAP_FIN 618, 720, 730, EA-FIN 617, 700, SAPSCORE 135, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 600, 602, 603, 604, 605, 606
- SAP BusinessObjects Business Intelligence Plate-forme versions ENTERPRISE 430, 2025, 2027
- SAP Human Capital Management pour SAP S/4HANA versions S4HCMRXX 100, 101, 102, SAP_HRRXX 600, 604, 608
- SAP Business Analytics et SAP Content Management version S4HCMRXX 100, 101, 102, SAP_HRRXX 600, 604, 608
- SAP S/4HANA OData Service version S4CORE 109
- SAP S/4HANA Backend OData Service version S4CORE 109
- SAP S/4HANA Frontend OData Service version UIS4H 109
- SAP Fournisseur Relationship Management versions SRM_SERVER 702, 713, 714
- SAP NetWeaver Application Server Java (Web Dynpro Java) version WD-RUNTIME 7.50

- SAP NetWeaver Application Server ABAP versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASE 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASE 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816
- SAP HANA Cockpit et HANA Database Explorer version SAP_HANA_COCKPIT 2.0
- SAP S/4HANA (Cloud privé et sur site) versions S4CORE 105, 106, 107, 108, 109, FI-CA 606, 616, 617, 618
- SAP Matériel Master Application versions S4CORE 102, 103, 104, 105, 106, 107, 108, 109, SCM_BASE 700, SCM_BASE 701, SCM_BASE 702, SCM_BASE 712, SCM_BASE 713, SCM_BASE 714
- SAP S4CORE versions S4CORE 104, 105, 106, 107, 108
- SAP Landscape Transformation versions DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020, S4CORE 102, 103, 104, 105, 106, 107, 108, 109

Identificateurs externes

- CVE-2026-27681; CVE-2026-34256; CVE-2025-64775; CVE-2026-34264; CVE-2026-34261;
- CVE-2026-27677; CVE-2026-27678; CVE-2026-27679; CVE-2026-0512; CVE-2026-27674;
- CVE-2026-34257; CVE-2026-34262; CVE-2026-27673; CVE-2026-27672; CVE-2026-27676;
- CVE-2025-42899; CVE-2026-24318; CVE-2026-27683; CVE-2026-27680; CVE-2026-27675.

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant les produits susmentionnés. L'exploitation de ces vulnérabilités pourrait permettre à un attaquant distant non authentifié d'exécuter du code arbitraire, de contourner les mécanismes d'authentification, d'accéder à des informations sensibles ou encore d'élever ses privilèges.

Solution

Veuillez se référer au bulletin de sécurité de SAP du 14 Avril 2026 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 ;
- Elévation de privilèges ;

Référence

Bulletin de sécurité SAP du 14 Avril 2026:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2026.html