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	60871002/26
Date de Publication	10 Février 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP NetWeaver AS ABAP & ABAP Platform (Noyau/Kernel) :
  - Versions KERNEL : 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.12, 9.14, 9.16, 9.17, 9.18, 9.19.
  - Versions KRNL64UC / KRNL64NUC : 7.22, 7.22EXT, 7.53, 8.04.
- SAP_BASIS : 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 804, 816, 916, 917, 918.
- SAP NetWeaver AS Java : Composant LMNWABASICAPPS 7.50.
- SAP NetWeaver JMS Service : Composant J2EE-FRMW 7.50.
- SAP Business Workflow : SAP_BASIS 752 à 816.
- SAP S/4HANA & ERP
- SAP CRM & S/4HANA (Scripting Editor) : S4FND (102 à 109), SAP_ABA 700, WEBCUIF (700 à 801).
- SAP S/4HANA Defense & Security : EA-DFPS (600 à 809).
- SAP Document Management System (DMS) : SAP_APPL 618, S4CORE (102 à 109), EA-APPL (600 à 617).
- SAP Fiori App (Manage Service Entry Sheets) : S4CORE (102 à 107).

- SAP Strategic Enterprise Management : SEM-BW (600 à 800).
- SAP BusinessObjects BI Platform : Versions ENTERPRISE 430, 2025 et 2027 (incluant AdminTools et Central Management Console).
- SAP Commerce Cloud : HY_COM 2205, COM_CLOUD 2211 (incluant JDK21).
- SAP Supply Chain Management (SCM) : SCM 700 à 712, SCMAPO 713 et 714.
- SAP Business One : Version 10.0 (B1_ON_HANA et SAP-M-BO).
- SAP Solution Tools / Support Tools (ST-PI) : Versions 2005_1_700, 2008_1_700/710, 740, 758.

Identificateurs externes

- CVE-2025-0059 CVE-2025-12383 CVE-2026-0484 CVE-2026-0485
- CVE-2026-0486 CVE-2026-0488 CVE-2026-0490 CVE-2026-0505
- CVE-2026-0508 CVE-2026-0509 CVE-2026-23681 CVE-2026-23684
- CVE-2026-23685 CVE-2026-23686 CVE-2026-23687 CVE-2026-23688
- CVE-2026-23689 CVE-2026-24312 CVE-2026-24319 CVE-2026-24320
- CVE-2026-24321 CVE-2026-24322 CVE-2026-24323 CVE-2026-24324
- CVE-2026-24325 CVE-2026-24326 CVE-2026-24327 CVE-2026-24328

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour de sécurité corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces failles pourrait permettre à un attaquant distant d'exécuter du code arbitraire, de contourner les mécanismes de sécurité, d'accéder à des informations confidentielles, d'élever ses privilèges ou encore de réaliser des injections SQL.

Solution

Veuillez se référer au bulletin de sécurité de SAP du 10 Février 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
- Injection SQL

Référence

Bulletin de sécurité SAP du 10 Février 2026:

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