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	61771003/26
Date de Publication	10 Mars 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP Quotation Management Insurance application (FS-QUO) Version FS-QU800.
- SAP NetWeaver Enterprise Portal Administration Version EP-RUNTIME 7.50.
- SAP Supply Chain Management (SCM) :
    - Version SCM 700, 701, 702, 712.
    - Versions SCMAP: 713, 714.
    - Versions S4CORE : 102, 103, 104.
    - Versions S4COREOP : 105, 106, 107, 108, 109.
- SAP NetWeaver Application Server for ABAP Versions SAP_BASIS : 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816, 918.
- SAP NetWeaver (Feedback Notification) Versions SAP_ABA : 700, 701, 702, 731, 740, 750, 751, 752, 75A, 75B, 75C, 75D, 75E, 75F, 75G, 75H, 75I, 816.
- SAP Business One (Job Service) Version B1_ON_HANA 10.0, SAP-M-B10.0.
- SAP Business Warehouse (Service API)
    - Versions DW4CORE : 200, 300, 400.
    - Versions PI_BASIS : 2006_1_700, 701, 702, 730, 731, 740.
    - Versions SAP_BW : 750, 751, 752, 753, 754, 755, 756, 757, 758, 816.

- SAP S/4HANA HCM Portugal & SAP ERP HCM Portugal :
    - Versions S4HCMCPT : 100, 101, 102.
    - Versions SAP_HRCPT : 600, 604, 608.
- SAP Customer Checkout 2.0 Version SAP_CUSTOMER_CHECKOUT 2.0.
- SAP GUI for Windows (avec GuiXT actif) Version BC-FES-GUI 8.00.
- SAP Solution Tools Plug-In (ST-PI) Version ST-PI 2008_1_700, 2008_1_710, 740, 758.
- SAP NetWeaver AS Java (Adobe Document Services) Version ADSSAP 7.50.

Identificateurs externes

- CVE-2019-17571 CVE-2025-9230 CVE-2025-9232 CVE-2026-0489 CVE-2026-24309
- CVE-2026-24310 CVE-2026-24311 CVE-2026-24313 CVE-2026-24316 CVE-2026-24317
- CVE-2026-27684 CVE-2026-27685 CVE-2026-27686 CVE-2026-27687 CVE-2026-27688
- CVE-2026-27689

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 provoquer un déni de service, 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 Mars 2026 afin d'installer les nouvelles mises à jour.

Risque

- Exécution du code arbitraire à distance ;
- Déni de service ;
- 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 Mars 2026:

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