ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits SAP
Numéro de Référence	56261308/25
Date de publication	13 Aout 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Business One (SLD) versions B1_ON_HANA 10.0 et SAP-M-BO 10.0
- Cloud Connector version SAP_CLOUD_CONNECTOR 2.0
- Fiori (Launchpad) version SAP_UI 754
- Landscape Transformation (Analysis Platform) versions DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020
- NetWeaver ABAP Platform versions S4CRM 100, 200, 204, 205, 206, S4CEXT 107, 108, 109, BBPCRM 713 et 714
- NetWeaver ABAP Platform versions SAP_BASIS 758, SAP_BASIS 816 et SAP_BASIS 916
- NetWeaver Application Server ABAP et ABAP Platform (Internet Communication Manager) versions KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.14, 9.15 et 9.16
- NetWeaver Application Server pour ABAP (BIC Document) versions S4COREOP 104, 105, 106, 107, 108, SEM-BW 600, 602, 603, 604, 605, 634, 736, 746, 747 et 748
- NetWeaver Application Server pour ABAP versions KRNL64UC 7.53, KERNEL versions 7.53, 7.54, 7.77, 7.89 et 7.93
- NetWeaver Application Server pour ABAP versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 816, SAP_BASIS 914 et SAP_BASIS 916
- S/4HANA (Bank Communication Management) Versions SAP_APPL 606, SAP_FIN 617, 618, 720, 730, S4CORE 102, 103, 104, 105, 106, 107 et 108

- S/4HANA avec le composant S4CORE versions 102, 103, 104, 105, 106, 107 et 108
- SAP GUI pour Windows version BC-FES-GUI 8.00

Identificateurs externes

CVE-2025-42934 CVE-2025-42935 CVE-2025-42936 CVE-2025-42941 CVE-2025-42942
CVE-2025-42943 CVE-2025-42945 CVE-2025-42946 CVE-2025-42948 CVE-2025-42949
CVE-2025-42950 CVE-2025-42951 CVE-2025-42955 CVE-2025-42957 CVE-2025-42975
CVE-2025-42976

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'injecter du contenu dans une page, d'exécuter du code arbitraire ou d'accéder à des données confidentielles.

Solution

Veuillez se référer au bulletin de sécurité de SAP afin d'installer les nouvelles mises à jour.

Risque

- Injection de de contenu dans une page
- Exécution de code arbitraire
- Accès à des données confidentielles

Référence

Bulletin de sécurité de SAP:

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