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 affectant plusieurs produits SAP
Numéro de Référence	52611202/25
Date de publication	12 Février 2025
Risque	Important
Impact	Important

Systèmes affectés

- GUI for Windows version BC-FES-GUI 8.00
- Supplier Relationship Management (Master Data Management Catalog) version SRM_MDM_CAT 7.52
- BusinessObjects Business Intelligence platform (Central Management Console) versions ENTERPRISE 430 et 2025
- Commerce versions HY_COM 2205 et COM_CLOUD 2211
- NetWeaver Application Server Java versions EP-BASIS 7.50 et FRAMEWORK-EXT 7.50
- Fiori for ERP versions SAP_GWFND 740, 750, 751, 752, 753, 754, 755, 756, 757 et 758
- Commerce (Backoffice) versions HY_COM 2205 et COM_CLOUD 2211
- NetWeaver AS Java (User Admin Application) version 7.50
- HANA extended application services, advanced model (User Account and Authentication Services) version SAP_EXTENDED_APP_SERVICES 1
- BusinessObjects Platform (BI Launchpad) versions ENTERPRISE 430 et 2025
- NetWeaver AS Java for Deploy Service versions ENGINEAPI 7.50 et SERVERCORE 7.50
- Fiori Apps Reference Library (My Overtime Requests) version GBX01HR5 605
- NetWeaver and ABAP platform (ST-PI) versions ST-PI 2008_1_700, ST-PI 2008_1_710 et ST-PI 740
- NetWeaver Application Server Java version WD-RUNTIME 7.50
- NetWeaver and ABAP Platform (SDCCN) versions ST-PI 2008_1_700, ST-PI 2008_1_710 et ST-PI 740
- Enterprise Project Connection version 3.0
- ABAP Platform (ABAP Build Framework) versions SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756,

SAP_BASIS 757 et SAP_BASIS 758

- NetWeaver Server 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 et SAP_BASIS 758

Identificateurs externes

CVE-2023-24527 CVE-2024-22126 CVE-2024-38819 CVE-2024-38820 CVE-2024-38828
CVE-2024-45216 CVE-2024-45217 CVE-2025-0054 CVE-2025-0064 CVE-2025-23187
CVE-2025-23189 CVE-2025-23190 CVE-2025-23191 CVE-2025-23193 CVE-2025-24867
CVE-2025-24868 CVE-2025-24869 CVE-2025-24870 CVE-2025-24872 CVE-2025-24874
CVE-2025-24875 CVE-2025-24876 CVE-2025-25241 CVE-2025-25243

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 un site, de contourner des mesures de sécurité 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
- Contournement de mesures de sécurité
- Accès à des données confidentielles

Référence

Bulletin de sécurité de SAP:

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