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	45991402/24
Date de publication	14 Février 2024
Risque	Important
Impact	Critique

Systèmes affectés

- SAP Business Client, Versions - 6.5, 7.0, 7.70
- SAP ABA (Application Basis), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75I
- SAP NetWeaver AS Java (User Admin Application), Version - 7.50
- SAP NetWeaver AS Java (Guided Procedures), Version - 7.50
- SAP CRM WebClient UI, Versions - S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, S4FND 108, WEBCUIF 700, WEBCUIF 701, WEBCUIF 730, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801
- IDES Systems, Versions – All version
- SAP Cloud Connector, Version - 2.0
- SAP GUI for Windows and SAP GUI for Java, Versions – SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758
- BAM (Bank Account Management), Versions – SAP_FIN 618, SAP_FIN 730, S4CORE 100, 101
- SAP Companion, Versions <3.1.38
- SAP NetWeaver Application Server ABAP (SAP Kernel), Versions - KERNEL 7.53, KERNEL 7.54, KERNESAP NWBC for HTML, Versions – SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731L 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.93, KERNEL 7.94, KRNL64UC 7.53
- SAP Fiori app ("My Overtime Requests"), Versions – 605
- SAP Master Data Governance Material, Versions – 618, 619, 620, 621, 622, 800, 801, 802, 803, 804
- SAP CRM (WebClient UI), Versions – S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 801
- SAP Master Data Governance, Versions - MDG_FND 731, MDG_FND 732, MDG_FND 746, MDG_FND 747, MDG_FND 748, MDG_FND 749, MDG_FND 752, MDG_FND 800, MDG_FND

802, MDG_FND 803, MDG_FND 804, MDG_FND 805, MDG_FND 806, MDG_FND 807, MDG_FND 808, SAP_BS_FND 702

Identificateurs externes

CVE-2023-31405 CVE-2023-44487 CVE-2023-49583 CVE-2023-50422
CVE-2023-50423 CVE-2023-50424 CVE-2024-21734 CVE-2024-21735 CVE-2024-21736
CVE-2024-21737 CVE-2024-21738 CVE-2024-22124 CVE-2024-22125

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 code et du contenu dans un site ou de contourner des mesures de sécurité.

Solution

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

Risque

- Injection de code dans une page
- Injection de de contenu dans une page
- Contournement de mesures de sécurité

Référence

Bulletin de sécurité de SAP:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/february-2024.html