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	45551201/24
Date de publication	12 Janvier 2024
Risque	Important
Impact	Important

Systèmes affectés

- Business Application Studio, Web IDE Full-Stack et Web IDE pour SAP HANA
- Edge Integration Cell versions supérieures ou égales à 8.9.13
- Business Technology Platform (BTP) Security Services Integration Libraries
- Application Interface Framework (File Adapter) version 702
- Web Dispatcher versions WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP 7.89, WEBDISP 7.90, WEBDISP 7.94 et WEBDISP 7.95
- NetWeaver AS ABAP et ABAP Platform versions KRNL64UC 7.53, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.94, KERNEL 7.93 et KERNEL 7.95
- Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge) version 1.0
- LT Replication Server versions S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107 et S4CORE 108
- S/4HANA Finance (Advanced Payment Management) versions SAPSCORE 128 et S4CORE 10
- NetWeaver AS for Java (Log Viewer) version ENGINEAPI 7.50, SERVERCORE 7.50 et J2EE-APPS 7.50
- NetWeaver ABAP Application Server et ABAP Platform 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 793 et SAP_BASIS 79
- NetWeaver (Internet Communication Manager) versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KRNL64NUC

7.22, KRNL64NUC 7.22_EXT, WEBDISP 7.22_EXT, WEBDISP 7.53 et WEBDISP 7.54
- Marketing (Contacts App) version 160

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'exécuter du code arbitraire ou de causer un déni de service.

Solution

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

Risque

- Exécution de code arbitraire à distance
- Déni de service

Référence

Bulletin de sécurité de SAP:

- https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=1

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma