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	42801207/23
Date de publication	12 Juillet 2023
Risque	Important
Impact	Important

Systèmes affectés

- SAP Business Client, Versions - 6.5, 7.0, 7.70
- SAP ECC and SAP S/4HANA (IS-OIL), Versions - 600, 602, 603,604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807
- SAP NetWeaver (BI CONT ADD ON), Versions – 707, 737, 747,757
- SAP Web Dispatcher, Versions – WEBDISP 7.49, WEBDISP7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85,WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49,KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00,SAP_EXTENDED_APP_SERVICES 1
- SAP UI5 Variant Management, Versions – SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200
- SAP SQL Anywhere, Version - 17.0
- SAP Web Dispatcher, Versions - WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP 7.89, WEBDISP 7.91, WEBDISP 7.92, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1
- SAP Solution Manager (Diagnostic Agent), Versions – 7.20
- SAP Solution Manager (Diagnostic Agent), Versions – 7.20
- SAP NetWeaver Process Integration (Runtime Workbench), Versions – SAP_XITOOL 7.50
- SAP NetWeaver Process Integration (Message Display Tool), Versions – SAP_XIAF 7.50

- SAP S/4HANA (Manage Journal Entry Template), Versions – S4CORE 104, 105, 106, 107
- SAP Enable Now, Version - WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704
- SAP NetWeaver AS ABAP and ABAP Platform, Version - KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL 7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93
- SAP BusinessObjects BI Platform (Enterprise), Version - 4.20, 430
- SAP NetWeaver AS for Java (Log Viewer), Version - ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50
- SAP ERP Defense Forces and Public Security, Version - 600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807
- SAP Business Warehouse and SAP BW/4HANA, Version -
- SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300

Identificateurs externes

CVE-2023-33992 CVE-2023-33987 CVE-2023-35874 CVE-2023-36917 CVE-2023-31405
CVE-2023-33990 CVE-2023-33989 CVE-2023-35871 CVE-2023-35870 CVE-2023-35873
CVE-2023-35872 CVE-2023-36921 CVE-2023-36922 CVE-2023-36924 CVE-2023-36925
CVE-2023-33991 CVE-2023-33988 CVE-2023-36918 CVE-2023-36920 CVE-2023-36919

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, de contourner le politique de sécurité, d'accéder à des données confidentielles 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
- Contournement de la politique de sécurité
- Accès à des données confidentielles
- Déni de service

Référence

Bulletin de sécurité de SAP:

- https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma