ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits SAP
Numéro de Référence	41341304/23
Date de Publication	13 Avril 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- ABAP Platform and SAP Web Dispatcher versions WEBDISP 7.85, 7.89, KERNEL 7.85, 7.89 et 7.91
- SAP Application Interface Framework (Custom Hint of Message Dashboard Application versions AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D et 75E
- SAP Application Interface Framework (Log Message View of Message Dashboard) versions AIF 703, AIFX 702, S4CORE 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D et 75E
- SAP Application Interface Framework (Message Monitoring and Message Monitoring for Administrators Application versions 600 et 700
- SAP Application Interface Framework (ODATA service) versions 755 et 756
- SAP Business Client versions 6.5, 7.0 et 7.70
- SAP BusinessObjects Business Intelligence Platform (Promotion Management versions 420 et 430
- SAP CRM (WebClient UI) versions S4FND 102, 103, 104, 105, 106, 107, WEBCUIF, 700, 701, 731, 730, 746, 747, 748, 800 et 801
- SAP CRM versions 700, 701, 702, 712 et 713
- SAP Commerce versions 1905, 2005 et 2011
- SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector) version 720
- SAP Fiori apps 1.0 for travel management in SAP ERP (My Travel Requests) version 600

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- SAP GUI for HTML versions KERNEL 7.22, 7.53, 7.547.77, 7.81, 7.85, 7.89, 7.91, KRNL64UC, 7.22, 7.22EXT, KRNL64UC 7.22 et 7.22EXT
- SAP HCM Fiori App My Forms (Fiori 2.0) version 605
- SAP Landscape Management version 3.0
- SAP NetWeaver (BI CONT ADDON) versions 707, 737, 747 et 757
- SAP NetWeaver AS Java for Deploy Service version 7.50
- SAP NetWeaver AS for ABAP (Business Server Pages) versions 700, 701, 702, 731, 740,750, 751, 752, 753, 754, 755, 756 et 757
- SAP NetWeaver AS for ABAP and ABAP Platform versions 740, 750, 751, 752, 753, 754, 755, 756, 757 et 791
- SAP NetWeaver Application Server for ABAP and ABAP Platform versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757 et 791
- SAP NetWeaver Enterprise Portal version 7.50
- SAP NetWeaver Process Integration version 7.50
- SAP Web Dispatcher and Internet Communication Manager versions KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22,7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21,7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.73, WEBDISP 7.53, 7.73, 7.77, 7.81, 7.82,7.83, KERNEL 7.21, 7.22,7.49, 7.53, 7.73, 7.77, 7.81, 7.82 et 7.83
- SapSetup (Software Installation Program) version 9.0

Identificateurs externes

- CVE-2023-27497 , CVE-2023-27267 , CVE-2022-41272 , CVE-2023-28765 , CVE-2023-27269 , CVE-2023-29186 , CVE-2023-26458 , CVE-2023-29187 , CVE-2023-28761 , CVE-2023-24528 , CVE-2023-28763 , CVE-2023-27499 , CVE-2023-27897 , CVE-2023-29189 , CVE-2021-33683 , CVE-2023-24527 , CVE-2023-29185 , CVE-2023-29108 , CVE-2020-13936 , CVE-2023-29109 , CVE-2023-1903 , CVE-2023-29110 , CVE-2023-29112 , CVE-2023-29111

Bilan de la vulnérabilité

SAP annonce la disponibilité d'une mise à jour de sécurité corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de porter atteinte à la confidentialité de données, de contourner la politique de sécurité, d'exécuter du code arbitraire à distance et de réussir une élévation de privilèges.

Solution

Veuillez se référer au bulletin de sécurité SAP du 12 Avril 2023**.**

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance
- Elévation de privilèges

Annexe

Bulletin de sécurité SAP 12 Avril 2023**:**

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