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	44831611/23
Date de Publication	16 Novembre 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- NetWeaver AS Java version 7.50
- Product-SAP ASE Cluster Edition version 15.7
- Product-SAP ASE versions 15.7, 16.0
- Product-SAP Event Stream Processor version 5.1
- Product-SAP IQ version 16.0
- Product-SAP Replication Server version 15.7
- Product-SAP SQL Anywhere versions 16.0, 17.0
- SAP Business One version 10.0
- SAP CommonCryptoLib version 8
- SAP NetWeaver AS ABAP, SAP NetWeaver AS Java et ABAP Platform of S/4HANA on-premise versions KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.22, KERNEL 8.04, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64UC 8.04, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT
- SAP NetWeaver AS Java version 7.5
- SAP NetWeaver Application Server ABAP et ABAP Platform versions KERNEL 722, KERNEL 7.53, KERNEL 7.77,KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.94, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT
- SAP Web Dispatcher versions 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89
- SAPContent Server versions 6.50, 7.53, 7.54

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

- SAPExtended Application Services et Runtime (XSA) versions SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00
- SAPHANA Database version 2.0
- SAPHost Agent version 722
- SAPSSOEXT version 17

Identificateurs externes

- CVE-2023-31403 CVE-2023-40309 CVE-2023-41366 CVE-2023-42477 CVE-2023-42480

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 causer un déni de service.

Solution

Veuillez se référer au bulletin de sécurité SAP du 14 Novembre 2023**.**

Risque

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

Annexe

Bulletin de sécurité SAP 14 Novembre 2023**:**

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