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	45201412/23
Date de publication	14 Décembre 2023
Risque	Important
Impact	Important

Systèmes affectés

- AP Business Client versions 6.5, 7.0 et 7.7
- Business Objects BI Platform versions 420 et 430
- Librairie @sap/xssec versions antérieures à 3.6.0
- Librairie cloud-security-services-integration-library versions 3.3.x antérieures à 3.3.0
- Librairie cloud-security-services-integration-library versions antérieures à 2.17.0
- Librairie github.com/sap/cloud-security-client-go versions antérieures à 0.17.0
- Librairie sap-xssec versions antérieures à 4.1.0
- SAP Biller Direct versions 635 et 750
- SAP BusinessObjects Web Intelligence version 420
- SAP Cloud Connector version 2.0
- SAP Commerce Cloud version 8.1
- SAP ECC et SAP S/4HANA (IS-OIL) versions 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806 et 807
- SAP ECC et SAP S/4HANA (IS-OIL) versions 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806 et 807
- SAP EMARSYS SDK ANDROID version 3.6.2
- SAP Fiori Launchpad versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, UI_700 200 et SAP_BASIS 793
- SAP GUI pour Windows et SAP GUI pour Java versions SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757 et SAP_BASIS 758
- SAP HCM (SMART PAYE solution) versions S4HCMCIE 100, SAP_HRCIE 600, SAP_HRCIE 604 et SAP_HRCIE 608

- SAP Master Data Governance versions 731, 732, 746, 747, 748, 749, 800, 751,752,801,802, 803, 804, 805, 806, 807 et 808
- SAP NetWeaver Application Server ABAP et ABAP Platform versions SAP_BASIS 700, SAP_BASIS731, SAP_BASIS740 et SAP_BASIS750
- SAP Solution Manager version 720
- SAPUI5 versions SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756 et UI_700 200
- SAP_BS_FND version 702

Identificateurs externes

CVE-2021-23413 CVE-2023-36922 CVE-2023-42476 CVE-2023-42478 CVE-2023-42479
CVE-2023-42481 CVE-2023-49058 CVE-2023-49577 CVE-2023-49578 CVE-2023-49580
CVE-2023-49581 CVE-2023-49583 CVE-2023-49584 CVE-2023-49587 CVE-2023-50422
CVE-2023-50423 CVE-2023-50424 CVE-2023-6542

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 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
- Déni de service

Référence

Bulletin de sécurité de SAP:

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