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	39531512/22
Date de publication	15 Décembre 2022
Risque	Important
Impact	Important

Systèmes affectés

- SAP Business Client versions 6.5, 7.0, 7.70
- SAP BusinessObjects Business Intelligence Platform versions 420, 430
- SAP NetWeaver Process Integration version 7.50
- SAP Commerce versions 1905, 2005, 2105, 2011, 2205
- SAP NetWeaver Process Integration version 7.50
- SAPBASIS versions 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, 791
- SAP Business Planning et Consolidation versions SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, DWCORE 200, 300, CPMBPC 8103229132
- SAP BusinessObjects Business Intelligence Platform (Program Objects) versions 420, 430
- SAP Commerce Webservices 2.0 (Swagger UI) versions 1905, 2005, 2105, 2011, 2205
- SAPUI5 CLIENT RUNTIME versions 600, 700, 800, 900, 1000
- SAPUI5 versions 754, 755, 756, 757
- SAP Disclosure Management version 10.1
- SAP NetWeaver AS pour Java (Http Provider Service) version 7.50
- SAP Solution Manager (Enterprise Search) versions 740, 750
- SAP NetWeaver AS ABAP (Business ServerPages Test Application IT00) versions 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757
- SAP Solution Manager (Diagnostic Agent) version 7.20
- SAP NetWeaver ABAP Server and ABAP Platform versions 700, 701, 702, 731, 740, 750-757, 789, 790
- SAP Business Objects Business Intelligence Platform (Web intelligence) versions 420, 430
- SAP Sourcing and SAP Contract Lifecycle Management version 1100

Identificateurs externes

CVE-2022-41267 CVE-2022-41272 CVE-2022-42889 CVE-2022-41271
CVE-2022-41264 CVE-2022-41268 CVE-2022-39013 CVE-2022-41266
CVE-2022-35737 CVE-2022-41274 CVE-2022-41262 CVE-2022-41275
CVE-2020-6215 CVE-2022-41261 CVE-2022-41215 CVE-2022-41263
CVE-2022-41273

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 contourner le politique de sécurité.

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

Référence

Bulletin de sécurité de SAP:

- https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=1&todaysdate=2022-12-14