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	40331602/23
Date de publication	16 Février 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Business Client versions 6.5, 7.0 et 7.70
- BusinessObjects Business Intelligence platform (Analysis edition for OLAP) versions 420 et 430
- BusinessObjects Business Intelligence platform (CMC) versions 420 et 430
- BusinessObjects Business Intelligence (Web Intelligence UI) version 430
- Business Planning and Consolidation versions 200 et 300
- Business Planning and Consolidation versions SAP_BW 750, 751, 752, 753, 754, 755, 756 et 757, DWCORE 200 et 300 et CPMBPC 810
- CRM (WebClient UI) versions 700, 701, 702, 731, 740, 750, 751 et 752, WEBCUIF 748, 800 et 801, S4FND 102 et 103
- Fiori apps 1.0 for travel management in SAP ERP (My Travel Requests) version 600
- GRC Process Control application versions GRCFND_A V1200, V8100, GRCPINW V1100_700, V1100_731 et V1200_750
- Host Agent Service versions 7.21 et 7.22
- NetWeaver Application Server for ABAP and ABAP Platform versions 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789 et 790
- NetWeaver AS ABAP and ABAP Platform versions 700, 701, 702, 731, 740, 750, 751 et 752
- NetWeaver AS ABAP (BSP Framework) version 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756 et 757
- NetWeaver AS ABAP (BSP Framework) version 700, 701, 702, 731 et 740
- NetWeaver AS ABAP (Business Server Pages application) versions 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G et 75H

- NetWeaver AS for ABAP and ABAP Platform version 702, 731, 740, 750, 751, 752, 753, 754, 755, 756 et 757
- NetWeaver AS for ABAP and ABAP Platform version 740, 750, 751, 752, 753, 754, 755, 756, 757, 789 et 790
- NetWeaver AS for ABAP and ABAP Platform versions 740, 750, 751, 752, 753, 754, 755, 756 et 757
- NetWeaver AS for Java (Http Provider Service) version 7.50
- S/4 HANA (Map Treasury Correspondence Format Data) versions 104 et 105
- SAPBASIS versions 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790 et 791
- Solution Manager (BSP Application) version 720
- Solution Manager version 720

Identificateurs externes

CVE-2022-41264	CVE-2023-23853	CVE-2023-0013	CVE-2022-41268
CVE-2022-41262	CVE-2023-0020	CVE-2023-0024	CVE-2023-0025
CVE-2023-23855	CVE-2023-0019	CVE-2023-23852	CVE-2023-23859
CVE-2023-23860	CVE-2023-23858	CVE-2023-23851	CVE-2023-23856
CVE-2023-23854	CVE-2023-24523	CVE-2023-24530	CVE-2023-24528
CVE-2023-24524	CVE-2023-24529	CVE-2023-25614	CVE-2023-24521
CVE-2023-24522	CVE-2023-24525		

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 d'accéder à des données confidentielles.

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

Référence

Bulletin de sécurité de SAP:

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

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