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	39711201/23
Date de publication	12 Janvier 2023
Risque	Important
Impact	Critique

Systèmes affectés

- SAP BPC MS 10.0 versions 800 et 810
- SAP BusinessObjects Business Intelligence platform versions 420 et 430
- SAP NetWeaver Process Integration version 7.50
- SAP BusinessObjects Business Intelligence Platform versions 4.2 et 4.3
- SAP NetWeaver Process Integration version 7.50
- SAP NetWeaver AS for Java version 7.50
- SAP NetWeaver ABAP Server et ABAP Platform versions SAP_BASIS 700, 701, 702,710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22 et 7.22EXT
- SAP Host Agent pour Windows versions 7.21 et 7.22
- SAP NetWeaver AS pour ABAP et ABAP Platform versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756 et 757
- SAP Bank Account Management versions 800 et 900

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, 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