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	43281008/23
Date de publication	10 Aout 2023
Risque	Important
Impact	Important

Systèmes affectés

- Host Agent, Version – 7.22
- SAP Business One (B1i Layer), Version – 10.0
- SAP Business Client, Versions - 6.5, 7.0, 7.70
- SAP Business One (Service Layer), Version – 10.0
- SAP Business One, Version – 10.0
- SAP BusinessObjects Business Intelligence (installer), Versions – 420, 430
- SAP BusinessObjects Business Intelligence Platform, Versions – 420
- SAP BusinessObjects Business Intelligence Platform, Versions – 430
- SAP Commerce (OCC API), Versions - HY_COM 2105, HY_COM 2205, COM_CLOUD 2211
- SAP Commerce, Versions – HY_COM 2105, HY_COM 2205, COM_CLOUD 2211
- SAP ECC and SAP S/4HANA (IS-OIL), Versions - 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807
- SAP Message Server, Versions – KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EX
- SAP NetWeaver AS ABAP and ABAP Platform, Versions – SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804
- SAP NetWeaver Process Integration, Versions - SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50

- SAP PowerDesigner, Version – 16.7
- SAP Supplier Relationship Management, Versions – 600, 602, 603, 604, 605, 606, 616, 617
- SAP NetWeaver (BI CONT ADD ON), Versions – 707, 737, 747, 757

Identificateurs externes

CVE-2023-33989 CVE-2023-33993 CVE-2023-36922 CVE-2023-36923 CVE-2023-36926
CVE-2023-37483 CVE-2023-37484 CVE-2023-37486 CVE-2023-37487 CVE-2023-37488
CVE-2023-37490 CVE-2023-37491 CVE-2023-37492 CVE-2023-39436 CVE-2023-39437
CVE-2023-39439 CVE-2023-39440

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, d'accéder à des données confidentielles 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
- Accès à des données confidentielles
- Déni de service

Référence

Bulletin de sécurité de SAP:

- https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html