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	34131201/22
Date de publication	12 Janvier 2021
Risque	Important
Impact	Critique

Systèmes affectés

- SAP Customer Checkout
- SAP BTP Cloud Foundry
- SAP Landscape Management
- SAP Connected Health Platform 2.0 - Fhirserver
- SAP HANA XS Advanced Cockpit
- SAP NetWeaver Process Integration
- SAP HANA XS Advanced
- SAP Internet of Things Edge Platform
- SAP BTP Kyma
- SAP Enable Now Manager
- SAP Cloud for Customer (complément pour le client Lotus notes)
- SAP Localization Hub, digital compliance service for India
- SAP Edge Services On Premise Edition
- SAP Edge Services Cloud Edition
- SAP BTP API Management (Tenant Cloning Tool)
- SAP NetWeaver ABAP Server and ABAP Platform (Adobe LiveCycle Designer 11.0)
- SAP Digital Manufacturing Cloud for Edge Computing
- SAP Enterprise Continuous Testing by Tricentis
- SAP Cloud-to-Cloud Interoperability
- SAP Reference Template for enabling ingestion and persistence of time series data in Azure
- SAP Business One

- SAP S/4HANA versions 100, 101, 102, 103, 104, 105 et 106
- SAP NetWeaver AS ABAP versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755 et 756
- SAP Business One version 10
- SAP Enterprise Threat Detection version 2.0
- SAP NetWeaver AS for ABAP and ABAP Platform versions 701, 702, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756 et 786
- SAP 3D Visual Enterprise Viewer version 9
- SAP GRC Access Control versions V1100_700, V1100_731 et V1200_750

Identificateurs externes

CVE-2021-44228	CVE-2021-44233	CVE-2021-44234	CVE-2021-44235
CVE-2022-22529	CVE-2022-22530	CVE-2022-22531	CVE-2022-42067
CVE-2021-42066	CVE-2021-42068	CVE-2021-42069	CVE-2021-42070

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités affectant certains de ses produits. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder à des informations confidentielles ou de causer un déni de service.

Solution

Veuillez-vous référer au bulletin de sécurité de SAP du mois de Janvier 2022 afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire à distance
- Accès à des informations confidentielles
- Déni de service

Référence

Bulletin de sécurité de SAP du mois de janvier 2022:

- https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=596902035