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 critiques affectant plusieurs produits SAP
Numéro de Référence	346900902/22
Date de publication	09 Février 2022
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP Web Dispatcher, Versions - 7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87
- SAP Content Server, Version - 7.53
- SAP NetWeaver and ABAP Platform, Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49
- SAP Commerce, Versions - 1905, 2005, 2105, 2011 Hot News 10
- SAP Data Intelligence, Version - 3
- SAP Dynamic Authorization Management, Version - 9.1.0.0, 2021.03 Hot News 10
- Internet of Things Edge Platform, Version - 4.0
- SAP Customer Checkout, Version - 2
- SAP Business Client, Version – 6.5 Hot News 10
- SAP Solution Manager (Diagnostics Root Cause Analysis Tools), Version - 720 Hot News 9.1
- SAP S/4HANA, Versions - 100, 101, 102, 103, 104, 105, 106 High 8.7
- SAP NetWeaver Application Server Java, Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53
- SAP NetWeaver AS ABAP (Workplace Server), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787 High 7.1
- SAP NetWeaver (ABAP and Java application Servers), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756
- SAP ERP HCM (Portugal), Versions - 600, 604, 608
- SAP Business Objects Web Intelligence (BI Launchpad) , Version - 420

- SAP 3D Visual Enterprise Viewer , Version - 9.0
- SAP Adaptive Server Enterprise , Version - 16.0
- SAP S/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer) , Versions - 104, 105, 106
- SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel) , Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49

Identificateurs externes

CVE-2021-44228	CVE-2021-45046	CVE-2021-45105	CVE-2021-44832
CVE-2022-22532	CVE-2022-22528	CVE-2022-22530	CVE-2022-22531
CVE-2022-22534	CVE-2022-22535	CVE-2022-22536	CVE-2022-22537
CVE-2022-22538	CVE-2022-22539	CVE-2022-22540	CVE-2022-22542
CVE-2022-22543	CVE-2022-22544	CVE-2022-22546	

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour permettant de corriger plusieurs vulnérabilités critiques 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 se référer au bulletin de sécurité de SAP du mois de Septembre 2021 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 Février 2022:

- https://wiki.scn.sap.com/wiki/display/PSR/SAP+Security+Patch+Day+-+February+2022