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	36371205/22
Date de publication	12 Mai 2022
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP Business One Cloud, Version -1.1
- SAP Commerce, Versions -1905, 2005, 2105 & 2011
- SAP Customer Profitability Analytics, Version -2
- SAP Webdispatcher, Versions -7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.83, 7.85
- SAP NetweaverASfor ABAP and Java (ICM), Versions -KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, 8.04, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 8.04
- SAP BusinessObjects Business Intelligence Platform, Versions -420, 430
- SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions -700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788
- SAP Employee Self Service (Fiori My Leave Request), Version -605
- SAP NetWeaver Application Server ABAP, Versions -753, 754, 755, 756
- SAP Host Agent, Version -7.22
- SAP NetWeaver and ABAPPlatform, Versions -KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.8
- SAP NetWeaver (ABAP and Java application Servers), Versions -700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756
- SAP NetWeaver ABAP Server and ABAP Platform, Versions -740, 750, 787

Identificateurs externes

CVE-2022-29611	CVE-2022-22541	CVE-2022-28214	CVE-2022-27656
CVE-2022-22965	CVE-2022-29613	CVE-2022-29610	CVE-2022-28774
CVE-2022-29616	CVE-2022-22534		

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 d'injecter du contenu dans une page.

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
- Accès à des informations confidentielles
- Injection de contenu dans une page

Référence

Bulletin de sécurité de SAP:

- https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=10