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	36891506/22
Date de publication	15 Juin 2022
Risque	Important
Impact	Important

Systèmes affectés

- SAP Business Client, Version -6.5
- SAP NetWeaver and ABAP Platform, Versions -KERNEL 7.49, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.49, KRNL64UC 7.49, SAP_ROUTER 7.53, 7.22
- SAP PowerDesigner Proxy 16.7, Versions -16.7
- SAP NetWeaver Application Server for ABAP and ABAP Platform,Version -700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788
- SAP 3D Visual Enterprise Viewer, Version -9.0
- SAP NetWeaver Development Infrastructure (Design Time Repository), Versions -7.30, 7.31, 7.40, 7.50
- SAP NetWeaver, ABAP Platform and SAP Host Agent, Versions -KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, 8.04, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, 8.04, SAPHOSTAGENT 7.22
- SAP ERP, localization forCEEcountries, Versions -C-CEE110_600, 110_602, 110_603, 110_604, 110_700
- SAP Financials, Versions -SAP_FIN 618, 720
- SAP S/4Hana Core, Versions -S4CORE 100, 101, 102, 103, 104, 105, 106, 107, 108
- SAP Adaptive Server Enterprise (ASE), Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53
- SAP NetWeaverASABAP,ASJava, ABAP Platform and HANA Database, Versions -KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.22,

7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, SAPHOSTAGENT 7.2
- SAP NetWeaver Developer Studio (NWDS), Versions -7.50
- SAP Adaptive Server Enterprise (ASE), Versions -KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53

Identificateurs externes

CVE-2022-29618 CVE-2022-27668 CVE-2022-29611 CVE-2022-29612
CVE-2022-31589 CVE-2022-29614 CVE-2022-31594

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'élever ses privilèges 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
- Elévation de privilèges
- 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