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	47821206/24
Date de publication	12 Juin 2024
Risque	Important
Impact	Critique

Systèmes affectés

- BW/4HANA Transformation et Data Transfer Process versions DW4CORE 200, 300, 400, 796, SAP_BW 740, 750, 751, 752, 753, 754, 755, 756, 757 et 758 sans le dernier correctif de sécurité
- Central Finance Infrastructure Components versions SAP_FIN 720, 730, SAPSCORE 114, S4CORE 100, 101 et 102 sans le dernier correctif de sécurité
- CRM WebClient UI versions S4FND 102, 103, 104, 105, 106, 107, WEBCUIF 700, 701, 730, 731, 746, 747, 748, 800 et 801 sans le dernier correctif de sécurité
- Document Builder versions S4CORE 100, 101, S4FND 102, 103, 104, 105, 106, 107, 108, SAP_BS_FND 702, 731, 746, 747 et 748 sans le dernier correctif de sécurité
- Financial Consolidation version FINANCE 1010 sans le dernier correctif de sécurité
- S/4HANA (Manage Incoming Payment Files) versions S4CORE 102, 103, 104, 105, 106, 107 et 108 sans le dernier correctif de sécurité
- SAP BusinessObjects Business Intelligence Platform versions ENTERPRISE 420, 430 et 440 sans le dernier correctif de sécurité
- SAP NetWeaver Application Server ABAP and ABAP Platform versions SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 795 et SAP_BASIS 796 sans le dernier correctif de sécurité
- SAP NetWeaver Application Server ABAP et ABAP Platform versions ST-PI 2008_1_700, 2008_1_710 et 740 sans le dernier correctif de sécurité
- SAP NetWeaver AS Java version GP-CORE 7.5 sans le dernier correctif de sécurité
- SAP NetWeaver AS Java version MMR_SERVER 7.5 sans le dernier correctif de sécurité

- Student Life Cycle Management versions IS-PS-CA 617, 618, 802, 803, 804, 805, 806, 807 et 808 sans le dernier correctif de sécurité

Identificateurs externes

CVE-2024-28164 CVE-2024-32733 CVE-2024-33001 CVE-2024-34683 CVE-2024-34684 CVE-2024-34686 CVE-2024-34688 CVE-2024-34690 CVE-2024-34691 CVE-2024-37176 CVE-2024-37177

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'injecter du code et du contenu dans un site, de contourner des mesures de sécurité et 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

- Injection de code dans une page
- Injection de de contenu dans une page
- Contournement de mesures de sécurité
- Déni de service

Référence

Bulletin de sécurité de SAP:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2024.html