ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans plusieurs produits SAP
Numéro de Référence	25851407/20
Date de Publication	14 juillet 2020
Risque	Important
Impact	Important

Systèmes affectés

- SAP Business Objects Business Intelligence Platform (BI Launchpad, CMC, bipodata, BI Launchpad, Web Intelligence HTML interface); Versions - 4.1, 4.2
- SAP Business Client, Version - 6.5;
- SAP NetWeaver (XML Toolkit for JAVA); Versions - ENGINEAPI 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50;
- SAP NetWeaver AS JAVA (IIOP service) (SERVERCORE); Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50;
- SAP NetWeaver AS JAVA (IIOP service) (CORE-TOOLS); Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50;
- SAP NetWeaver (ABAP Server) et ABAP Platform; Versions - 731, 740, 750
- SAP Disclosure Management ; Version - 1.0;

Identificateurs externes

- CVE-2020-6285, CVE-2020-6267, CVE-2020-6281, CVE-2020-6276;
- CVE-2020-6278, CVE-2020-6222, CVE-2020-6280, CVE-2020-6282;

Bilan de la vulnérabilité

SAP annonce la disponibilité de mises à jour de sécurité qui corrigent des vulnérabilités affectant certains de ses produits. L'exploitation de ces failles peut permettre à un attaquant d'exécuter du code arbitraire à distance, de réussir une élévation de privilèges et de prendre le contrôle du système affecté.

Solution

Veuillez-vous référer au bulletin de sécurité SAP du 14 Juillet 2020 afin d'installer les nouvelles mises à jour.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risque

- Exécution de code arbitraire à distance ;
- Prise de contrôle du système affecté ;
- Elévation de privileges;

Référence

Bulletin de sécurité SAP du 14 Juillet 2020 :

- https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675