



BULLETIN DE SECURITE

Titre : Vulnérabilités dans plusieurs produits SAP

Numéro de Référence : 22461511/19

Risque : Important

Impact : Important

Systemes affectés

- SAP Business Client, Version - 6.5
- SAP Diagnostic Agent (LM-Service), Version - 7.20
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), Versions - 4.1, 4.2
- SAP Enable Now, Versions – antérieure à 1908
- S4HANA Sales (S4CORE), Versions - 1.0, 1.01, 1.02, 1.03, 1.04
- SAP Treasury and Risk Management (S4CORE), Versions - 1.01, 1.02, 1.03, 1.04
- SAP Treasury and Risk Management (EA-FINSERV), Versions - 6.0, 6.03, 6.04, 6.05, 6.06, 6.16, 6.17, 6.18, 8.0
- SAP NetWeaver Application Server Java (J2EE-Framework), Versions - 7.1, 7.2, 7.3, 7.31, 7.4, 7.5
- SAP BusinessObjects Business Intelligence Platform (Web Intelligence), Versions - 4.2
- SAP Quality Management (S4CORE), Versions - 1.0, 1.01, 1.02, 1.03
- SAP Diagnostics Agent (LM_Service), Versions - 7.2
- SAP UI, Versions - 7.5, 7.51, 7.52, 7.53, 7.54
- SAP UI 700, Versions - 2.0
- SAP NetWeaver AS Java, Versions - 7.10, 7.20, 7.30, 7.31, 7.4, 7.5
- SAP Treasury and Risk Management (S4CORE), Versions - 1.01, 1.02, 1.03, 1.04

Identificateurs externes

- CVE-2019-0330, CVE-2019-0396 CVE-2019-0385 CVE-2019-0386 CVE-2019-0384
- CVE-2019-0389 CVE-2019-0382 CVE-2019-0393 CVE-2019-0390 CVE-2019-0388
- CVE-2019-0391 CVE-2019-0383

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits SAP. L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code arbitraire à distance, de causer un déni de service, de réussir une élévation de privilèges et de prendre le contrôle du système affecté.

Solution :

Veillez-vous référer au bulletin de sécurité SAP du 12 Novembre 2019 afin d'installer les nouvelles mises à jour:

Risque :

- Exécution de code arbitraire à distance,
- Perte de contrôle du système affecté.
- Déni de service
- Elévation de privilèges.

Référence :

Bulletin de sécurité SAP du 12 novembre 2019

<https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=528880390>