



BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits SAP
Numéro de Référence	39161011/22
Date de Publication	10 Novembre 2022
Risque	Critique
Impact	Critique

Systemes affectés

- SAP BusinessObjects Business Intelligence Platpoum (Central Management Console et BI Launchpad), Versions -4.2, 4.3
- SAPUI5 CLIENT RUNTIME, Versions –600, 700, 800, 900, 1000
- SAPUI5, Versions –754, 755, 756, 757
- SAP Commerce, Versions -1905, 2005, 2105, 2011, 2205
- SAP NetWeaver Application Server ABAP et ABAP Platpoum, Versions-700, 731, 804, 740, 750, 789
- SAP SuccessFactors attachmentAPIpour Mobile Application (etroid &iOS), Versions - <8.1.2
- SAP 3D Visual Enterprise Author, Version –9.0
- SAP 3D Visual Enterprise Viewer, Version –9.0
- SAP Financial Consolidation, Version -1010
- SAP Biller Direct, Versions-635, 750
- SAP GUI pour Windows, Version –7.70
- SAP NetWeaver ABAP Server et ABAP Platpoum, Versions-700, 731, 740, 750, 789

Identificateurs externes

- CVE-2022-41203 , CVE-2021-20223 , CVE-2022-35737 , CVE-2022-41204 , CVE-2022-41214 , CVE-2022-35291 , CVE-2022-41211 , CVE-2022-41259 , CVE-2022-41258 , CVE-2022-41260, CVE-2022-41208 , CVE-2022-41207 , CVE-2022-41205 , CVE-2022-41215

Bilan de la vulnérabilité

SAP annonce la disponibilité d'une mise à jour de sécurité corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. L'exploitation de ces failles peut permettre à un attaquant de porter atteinte à la confidentialité de données, de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

Solution

Veillez se référer au bulletin de sécurité SAP du 08 Novembre 2022.

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Exécution du code arbitraire à distance

Annexe

Bulletin de sécurité Microsoft 08 Novembre 2022:

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