



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits SAP
Numéro de Référence	50691211/24
Date de Publication	12 Novembre 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- SAP Bank Account Management, Version - 100, 101, 102, 103, 104, 105, 106, 107, 108
- SAP Cash Management (Cash Operations), Version - S4CORE 103, 104, 105, 106, 107, 108
- SAP NetWeaver Application Server pour ABAP, Versions – KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12
- SAP NetWeaver Java (Software Update Manager), Versions - SUM 1.1
- SAP Host Agent, Version – SAPHOSTAGENT 7.22
- SAP NetWeaver AS Java (System Landscape Directory), Versions – LM-SLD 7.5
- SAP NetWeaver Application Server Java (Logon Application), Versions – SERVER-CORE 7.5
- SAP PDCE, Version – S4CORE 102, 103, S4COREOP 104, 105, 106, 107, 108
- SAP Web Dispatcher, Versions – WEBDISP 7.77, 7.89, 7.93, KERNEL 7.77, 7.89, 7.93, 9.12, 9.13

Identificateurs externes

- CVE-2024-33000 CVE-2024-39592 CVE-2024-42372 CVE-2024-47586 CVE-2024-47587 CVE-2024-47588 CVE-2024-47590 CVE-2024-47592 CVE-2024-47593 CVE-2024-47595

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 et de causer un déni de service

Solution

Veillez se référer au bulletin de sécurité SAP du 12 Novembre 2024.

Risque

- Accès aux informations confidentielles
- Contournement de la politique de sécurité
- Dénî de service

Annexe

Bulletin de sécurité SAP 12 Novembre 2024:

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