



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits SAP
Numéro de Référence	57421410/25
Date de publication	14 octobre 2025
Risque	Critique
Impact	Critique

Systemes affectés

- SAP NetWeaver AS Java Version - SERVERCORE 7.50
- SAP Print Service Versions - SAPSPRINT 8.00, 8.10
- SAP Supplier Relationship Management Versions - SRMNXPO1 100, 150
- SAP Commerce Cloud Versions - HY_COM 2205, COM_CLOUD 2211, 2211-JDK21
- SAP Data Hub Integration Suite Version - CX_DATAHUB_INT_PACK 2205
- SAP NetWeaver Application Server ABAP Versions – KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.12, 9.14
- SAP Application Server for ABAP Versions - SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, 816
- SAP NetWeaver Application Server for ABAP Versions - KRNL64UC 7.53, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93, 9.16
- SAP Commerce Cloud Version - COM_CLOUD 2211
- SAP NetWeaver AS ABAP and ABAP Platform Versions - KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 9.14, 9.15, 9.16
- SAP S/4HANA Versions - S4CORE 104, 105, 106, 107, 108, 109
- SAP NetWeaver Versions - SAP_ABA 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H, 75I
- SAP Financial Service Claims Management Versions - INSURANCE 803, 804, 805, 806, S4CEXT 107, 108, 109
- SAP BusinessObjects Versions - ENTERPRISE 430, 2025, 2027
- SAP Cloud Appliance Library Appliances Version - TITANIUM_WEBAPP 4.0

Identificateurs externes

CVE-2025-0059	CVE-2025-31331	CVE-2025-31672	CVE-2025-42901	CVE-2025-42902
CVE-2025-42903	CVE-2025-42906	CVE-2025-42908	CVE-2025-42909	CVE-2025-42910
CVE-2025-42937	CVE-2025-42939	CVE-2025-42944	CVE-2025-48913	CVE-2025-5115

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, de contourner des mesures de sécurité, d'accéder à des données confidentielles ou 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
- Contournement de mesures de sécurité
- Accès à des données confidentielles
- Déni de service

Référence

Bulletin de sécurité de SAP:

- <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2025.html>