



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant plusieurs produits SAP
Numéro de Référence	59971501/26
Date de publication	15 janvier 2026
Risque	Critique
Impact	Critique

Systemes affectés

- Wily Introscope Enterprise Manager (WorkStation) version WILY_INTRO_ENTERPRISE 10.8
- Fiori App (Intercompany Balance Reconciliation) versions UIAPFI70 500, 600, 700, 800, 900, 901, 902, S4CORE 102, 103, 104, 105, 106, 107 et 108
- Fiori App (Intercompany Balance Reconciliation) versions UIAPFI70 500, 600, 700, 800, 900, 901, 902, S4CORE 102, 103, 104, 105, 106, 107, 108, 109 et UIS4H 109
- Fiori App (Intercompany Balance Reconciliation) versions UIAPFI70 500, 600, 700, 800, 900, 901, 902 et UIS4H 109
- HANA database version HDB 2.00
- Business Connector version SAP BC 4.8
- NetWeaver Enterprise Portal version EP-RUNTIME 7.50
- NetWeaver Enterprise Portal version EP-RUNTIME 7.50
- S/4HANA Private Cloud and On-Premise (Financials General Ledger) versions S4CORE 102, 103, 104, 105, 106, 107, 108 et 109
- NW AS Java UME User Mapping versions ENGINEAPI 7.50, SERVERCORE 7.50 et UMEADMIN 7.50
- Landscape Transformation versions DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752 et 2020
- S/4HANA Private Cloud and On-Premise (Financials General Ledger) versions S4CORE 102, 103, 104, 105, 106, 107, 108 et 109
- Identity Management versions IDM_CLM_REST_API 8.0 et IDMIC 8.0
- NetWeaver Application Server ABAP et ABAP Platform versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750,

- SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 et SAP_BASIS 816
- Supplier Relationship Management (SICF Handler in SRM Catalog) versions SRM_SERVER 700, 701, 702, 713 et 714
 - Fiori App (Intercompany Balance Reconciliation) versions UIAPFI70 500, 600, 700, 800, 900, 901, 902, S4CORE 102, 103, 104, 105, 106, 107, 108, 109 et UIS4H 109
 - NW AS Java UME User Mapping versions ENGINEAPI 7.50, SERVERCORE 7.50 et UMEADMIN 7.50
 - ERP Central Component and S/4HANA (EHS Management) versions SAP_APPL 618, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 605, 606 et 617
 - Business Server Pages Application (Product Designer Web UI) versions SAP_APPL 618, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 600, 602, 603, 604, 605, 606 et 617
 - Business Server Pages Application (Product Designer Web UI) versions SAP_APPL 618, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 600, 602, 603, 604, 605, 606 et 617
 - Supplier Relationship Management (SICF Handler in SRM Catalog) versions SRM_SERVER 700, 701, 702, 713 et 714
 - Landscape Transformation versions DMIS 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2018_1_752 et 2020
 - S/4HANA (Private Cloud and On-Premise) versions S4CORE 102, 103, 104, 105, 106, 107, 108 et 109
 - Wily Introscope Enterprise Manager (WorkStation) version WILY_INTRO_ENTERPRISE 10.8
 - Application Server for ABAP and NetWeaver RFCSDK versions KRNL64UC 7.53, NWRFCSDK 7.50, KERNEL 7.53, 7.54, 7.77, 7.89, 7.93 et 9.16
 - NetWeaver Application Server ABAP et ABAP Platform versions SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 et SAP_BASIS 816
 - Business Connector version SAP BC 4.8
 - S/4HANA (Private Cloud and On-Premise) versions S4CORE 102, 103, 104, 105, 106, 107, 108 et 109
 - Fiori App (Intercompany Balance Reconciliation) versions UIAPFI70 500, 600, 700, 800, 900, 901, 902 et UIS4H 109
 - HANA database version HDB 2.00
 - ERP Central Component and S/4HANA (EHS Management) versions SAP_APPL 618, S4CORE 102, 103, 104, 105, 106, 107, 108, 109, EA-APPL 605, 606 et 617
 - Fiori App (Intercompany Balance Reconciliation) versions UIAPFI70 500, 600, 700, 800, 900, 901, 902, S4CORE 102, 103, 104, 105, 106, 107 et 108
 - Identity Management versions IDM_CLM_REST_API 8.0 et IDMIC 8.0

Identificateurs externes

CVE-2026-0491	CVE-2026-0492	CVE-2026-0493	CVE-2026-0494	CVE-2026-0495
CVE-2026-0496	CVE-2026-0497	CVE-2026-0498	CVE-2026-0499	CVE-2026-0500

CVE-2026-0501	CVE-2026-0503	CVE-2026-0504	CVE-2026-0506	CVE-2026-0507
CVE-2026-0510	CVE-2026-0511	CVE-2026-0513	CVE-2026-0514	

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, d'élever ses privilèges, ou d'injecter du code SQL.

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
- Elévation de privilèges
- Injection de code SQL

Référence

Bulletin de sécurité de SAP:

- <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2026.html>