Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0006

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-01-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

SAP heeft kwetsbaarheden verholpen in SAP S/4HANA (Private Cloud en On-Premise), SAP Wily Introscope Enterprise Manager, SAP Landscape Transformation, SAP HANA, SAP Application Server voor ABAP, SAP NetWeaver, SAP ECC, SAP Fiori App voor Intercompany Balance Reconciliation, SAP NetWeaver Application Server ABAP, SAP Business Connector, SAP Supplier Relationship Management, SAP Identity Management, en SAP User Management Engine.

Duiding

De kwetsbaarheden variëren van SQL-injectie en OS-commando-injectie tot privilege-escalatie en Cross-Site Scripting (XSS). Aanvallers kunnen deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te verkrijgen, gegevensintegriteit in gevaar te brengen, of zelfs volledige systeemcompromittering te veroorzaken. De impact op de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen is aanzienlijk, vooral voor producten zoals SAP S/4HANA en SAP HANA, waar aanvallers met admin-rechten schadelijke ABAP-code kunnen injecteren. Andere kwetsbaarheden, zoals onvoldoende autorisatiecontroles in SAP Fiori Apps, kunnen leiden tot privilege-escalatie en ongeautoriseerde toegang tot gevoelige informatie.

Oplossingen

SAP heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-0501	5.3 MEDIUM
CVE-2026-0500	8.7 HIGH
CVE-2026-0498	8.6 HIGH
CVE-2026-0491	8.6 HIGH
CVE-2026-0492	8.7 HIGH

CVE-2026-0507	8.5 HIGH
CVE-2026-0511	5.3 MEDIUM
CVE-2026-0506	5.3 MEDIUM
CVE-2026-0503	5.3 MEDIUM
CVE-2026-0499	5.3 MEDIUM
CVE-2026-0514	5.3 MEDIUM
CVE-2026-0513	5.3 MEDIUM
CVE-2026-0494	5.3 MEDIUM
CVE-2026-0493	5.3 MEDIUM
CVE-2026-0497	5.3 MEDIUM
CVE-2026-0504	5.1 MEDIUM
CVE-2026-0510	2.1 LOW

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-306	Missing Authentication for Critical Function
CWE-326	Inadequate Encryption Strength
CWE-352	Cross-Site Request Forgery (CSRF)

CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-862	Missing Authorization
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

SAP
Application Server for ABAP and NetWeaver RFCSDK
Business Server Pages Application
ERP Central Component and S4HANA
Fiori App
HANA Database
Identity Management
Landscape Transformation
NW AS Java UME User Mapping
NetWeaver Application Server ABAP and ABAP Platform
NetWeaver Enterprise Portal
S4HANA

S4HANA Private Cloud and On-Premise
SAP NetWeaver Application Server ABAP and ABAP Platform
SAP NetWeaver Enterprise Portal
SAP Software
Supplier Relationship Management
Wily Introscope Enterprise Manager

Disclaimer