Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0140

Kwetsbaarheden verholpen in diverse SAP-producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-05-2026

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, SAP Commerce Cloud, SAP Forecasting & Replenishment, SAP NetWeaver Application Server voor ABAP, SAP Business Server Pages, SAP BusinessObjects Business Intelligence Platform, SAP Strategic Enterprise Management Scorecard Wizard, SAPUI5 Search UI, SAP Financial Consolidation, SAP Incentive and Commission Management, SAP Application Server ABAP voor SAP NetWeaver en ABAP Platform, en SAP HANA Deployment Infrastructure.

Duiding

De kwetsbaarheden betreffen verschillende typen beveiligingsproblemen binnen de genoemde SAP-producten.

- In SAP S/4HANA's Enterprise Search for ABAP module kunnen geauthenticeerde aanvallers SQL-injecties uitvoeren, wat kan leiden tot ongeautoriseerde toegang tot gevoelige data en applicatiecrashes.
- SAP Commerce Cloud bevat een configuratiefout in Spring Security waardoor ongeauthenticeerde gebruikers kwaadaardige configuraties kunnen uploaden en daarmee willekeurige server-side code kunnen uitvoeren.
- In SAP Forecasting & Replenishment en SAP NetWeaver Application Server voor ABAP kunnen geauthenticeerde gebruikers met administratieve rechten OS-commando's uitvoeren, wat kan resulteren in systeemcompromittering of verstoring van de applicatie.
- SAP S/4HANA Condition Maintenance heeft een ontbrekende autorisatiecontrole waardoor geauthenticeerde gebruikers records kunnen bekijken en wijzigen zonder de juiste permissies.
- SAP Business Server Pages Application component TAF_APPLAUNCHER en SAP NetWeaver Application Server ABAP bevatten Cross-Site Scripting (XSS) kwetsbaarheden die het mogelijk maken om gebruikers te misleiden via kwaadaardige links.
- SAP BusinessObjects Business Intelligence Platform heeft een Cross Site Request Forgery (CSRF) kwetsbaarheid die geauthenticeerde gebruikers kan misleiden tot het uitvoeren van ongewenste acties.
- SAP Strategic Enterprise Management Scorecard Wizard kent een autorisatiefout waardoor geauthenticeerde gebruikers toegang krijgen tot niet-toegestane informatie en instellingen kunnen wijzigen.
- SAPUI5 Search UI is kwetsbaar voor URL-parameter manipulatie die kan leiden tot het injecteren van kwaadaardige content en gebruikers kan omleiden naar aanvallersites.
- SAP Financial Consolidation bevat een kwetsbaarheid waarmee geauthenticeerde gebruikers sessies van andere gebruikers kunnen beëindigen, wat de beschikbaarheid beïnvloedt.
- SAP Incentive and Commission Management heeft onvoldoende autorisatiecontrole waardoor geauthenticeerde gebruikers database tabellen kunnen aanpassen.
- SAP Application Server ABAP voor SAP NetWeaver en ABAP Platform bevat een code-injectie kwetsbaarheid die geauthenticeerde gebruikers kunnen misbruiken om willekeurige code uit te voeren.
- SAP HANA Deployment Infrastructure bevat een SQL-injectie kwetsbaarheid in de @sap/hdi-deploy package, waarbij gebruikers met hoge privileges dynamische SQL-query's kunnen manipuleren, wat de vertrouwelijkheid en beschikbaarheid kan beïnvloeden.

Daarnaast is er een gerelateerde kwetsbaarheid in Apache Log4j Core (versies 2.0-beta9 tot 2.25.2) met ontbrekende TLS hostname verificatie, die man-in-the-middle aanvallen mogelijk maakt en ook diverse SAP-producten en andere software beïnvloedt.

Oplossingen

SAP heeft updates uitgebracht om de kwetsbaarheden in de genoemde producten te verhelpen. Daarnaast zijn er updates voor Apache Log4j beschikbaar (versies 2.18.0, 2.19.0 en 2.20.0) die de ontbrekende TLS hostname verificatie en andere problemen adresseren. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-34260	5.3 MEDIUM
CVE-2026-34263	8.7 HIGH
CVE-2026-34259	8.4 HIGH
CVE-2026-40135	5.1 MEDIUM
CVE-2026-40133	5.3 MEDIUM
CVE-2026-40137	5.3 MEDIUM
CVE-2026-0502	5.3 MEDIUM
CVE-2026-40132	5.3 MEDIUM
CVE-2025-68161	6.3 MEDIUM
CVE-2026-34258	5.3 MEDIUM
CVE-2026-27682	5.3 MEDIUM
CVE-2026-40136	5.3 MEDIUM

CVE-2026-40134	**5.3 MEDIUM**
CVE-2026-40129	**5.3 MEDIUM**
CVE-2026-40131	**5.1 MEDIUM**

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-459	Incomplete Cleanup
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-404	Improper Resource Shutdown or Release
CWE-451	User Interface (UI) Misrepresentation of Critical Information
CWE-862	Missing Authorization
CWE-937	OWASP Top Ten 2013 Category A9 - Using Components with Known Vulnerabilities
CWE-1035	OWASP Top Ten 2017 Category A9 - Using Components with Known Vulnerabilities

Getroffen producten

SAP
Application Server ABAP for NetWeaver and ABAP Platform
Business Server Pages Application
BusinessObjects Business Intelligence Platform
Commerce Cloud Configuration
Financial Consolidation
Forecasting & Replenishment
HANA Deployment Infrastructure deploy library
Incentive and Commission Management
NetWeaver Application Server ABAP
NetWeaver Application Server for ABAP and ABAP Platform
S4HANA
S4HANA Condition Maintenance
SAP BusinessObjects Business Intelligence Platform
SAP Financial Consolidation
SAP NetWeaver Application Server for ABAP and ABAP Platform

SAP Software
Strategic Enterprise Management
UI5
netweaver_application_server_abap

Disclaimer