Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0395

Kwetsbaarheden verholpen in SAP Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-12-2025

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 meerdere kwetsbaarheden verholpen in verschillende producten, waaronder SAP Solution Manager, SAP jConnect, SAP Web Dispatcher, SAP NetWeaver, SAP S/4 HANA Private Cloud, en SAP BusinessObjects.

Duiding

De kwetsbaarheden omvatten onder andere code-injectie, deserialisatie, en onvoldoende invoervalidatie, die kunnen leiden tot ongeautoriseerde toegang, gegevensverlies, en verstoring van de beschikbaarheid van systemen. Aangevallen systemen kunnen ernstige gevolgen ondervinden, zoals het uitvoeren van kwaadaardige code door geauthenticeerde aanvallers, en het risico op gegevenslekken door onvoldoende autorisatiecontroles. De impact op de vertrouwelijkheid, integriteit en beschikbaarheid van de systemen is aanzienlijk, met name voor de SAP producten die kwetsbaar zijn voor Denial-of-Service aanvallen en andere exploitatievormen.

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/december-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-42880	8.7 HIGH
CVE-2025-55754	2.1 LOW
CVE-2025-42928	8.6 HIGH
CVE-2025-42878	2.3 LOW
CVE-2025-42874	7.9 HIGH
CVE-2025-48976	8.7 HIGH
CVE-2025-42877	8.7 HIGH

CVE-2025-42876	5.3 MEDIUM
CVE-2025-42875	5.1 MEDIUM
CVE-2025-42904	5.3 MEDIUM
CVE-2025-42872	5.3 MEDIUM
CVE-2025-42873	8.2 HIGH
CVE-2025-42891	5.1 MEDIUM
CVE-2025-42896	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-116	Improper Encoding or Escaping of Output
CWE-150	Improper Neutralization of Escape, Meta, or Control Sequences
CWE-306	Missing Authentication for Critical Function
CWE-404	Improper Resource Shutdown or Release
CWE-405	Asymmetric Resource Consumption (Amplification)
CWE-489	Active Debug Code
CWE-502	Deserialization of Untrusted Data
CWE-549	Missing Password Field Masking
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-862	Missing Authorization
CWE-937	CWE-937

CWE-1035	CWE-1035
CWE-1244	Internal Asset Exposed to Unsafe Debug Access Level or State

Getroffen producten

SAP
Application Server ABAP
BusinessObjects Business Intelligence Platform
Enterprise Search for ABAP
NetWeaver Enterprise Portal
NetWeaver Internet Communication Framework
S4 HANA Private Cloud
SAPUI5, OpenUI5
Solution Manager
Web Dispatcher and Internet Communication Manager
Web Dispatcher, Internet Communication Manager and Content Server
jConnect

Disclaimer