Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0186

Kwetsbaarheden verholpen in SAP Producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-06-2025

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 kwetsbaarheden verholpen in diverse SAP producten als HANA, Business Objects en Netweaver.

Duiding

De kwetsbaarheden omvatten een gebrek aan autorisatiecontroles, waardoor aanvallers functies zonder beperkingen kunnen uitvoeren. Dit kan leiden tot ongeautoriseerde acties binnen de applicatie, wat de integriteit en vertrouwelijkheid in gevaar kan brengen. Daarnaast zijn er kwetsbaarheden die het mogelijk maken voor geauthenticeerde gebruikers om hun privileges te escaleren, wat kan resulteren in een significante compromittering van de applicatie. De aanwezigheid van Cross-Site Scripting (XSS) kwetsbaarheden stelt aanvallers in staat om kwaadaardige scripts op te slaan, wat de vertrouwelijkheid van gevoelige sessie-informatie in gevaar kan brengen. De noodzaak voor verbeterde beveiligingsmaatregelen en strikte toegangcontroles is duidelijk.

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/june-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-42984	5.3 MEDIUM
CVE-2025-42998	6.9 MEDIUM
CVE-2025-42987	5.3 MEDIUM
CVE-2025-42989	5.3 MEDIUM
CVE-2025-42982	8.7 HIGH
CVE-2025-42983	5.3 MEDIUM

CVE-2025-23192	5.1 MEDIUM
CVE-2025-42977	5.1 MEDIUM
CVE-2025-42994	8.7 HIGH
CVE-2025-42993	5.1 MEDIUM
CVE-2025-31325	5.3 MEDIUM
CVE-2025-42991	5.3 MEDIUM
CVE-2025-42988	6.3 MEDIUM
CVE-2025-42990	2.1 LOW

CWE's

CWE	Beschrijving
CWE-590	Free of Memory not on the Heap
CWE-862	Missing Authorization
CWE-346	Origin Validation Error
CWE-918	Server-Side Request Forgery (SSRF)
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

SAP
NetWeaver
NetWeaver Application Server for ABAP

SAP GRC (AC Plugin)
Business Warehouse and Plug-In Basis
BusinessObjects Business Intelligence
NetWeaver Visual Composer
MDM Server
SAP S/4HANA (Enterprise Event Enablement)
SAP NetWeaver (ABAP Keyword Documentation)
SAP S/4HANA (Manage Central Purchase Contract application)
Business One Integration Framework
SAP S/4HANA (Manage Processing Rules - For Bank Statement)
Business Objects Business Intelligence Platform
SAPUI5 applications

Disclaimer