Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0245

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 05-09-2025
Revisie: 1.0.1

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

Update Revisie 1

Er worden meldingen gemaakt dat de kwetsbaarheid met kenmerk CVE-2025-42957 wordt misbruikt.

Feiten

SAP heeft kwetsbaarheden verholpen in verschillende producten, waaronder in SAP NetWeaver Application Server ABAP, SAP S/4HANA, SAP Landscape Transformation en AP Cloud Connector.

Duiding

De kwetsbaarheden omvatten onder andere het omzeilen van autorisatiecontroles, Cross-Site Scripting (XSS) en een Directory Traversal kwetsbaarheid. De aanwezigheid van Cross-Site Scripting (XSS) en CRLF-injectie kwetsbaarheden stelt aanvallers in staat om sessies te manipuleren en gevoelige informatie te compromitteren.

Van de kwetsbaarheid met kenmerk CVE-2025-42957 wordt gemeld dat deze beperkt actief is misbruikt. Misbruik vereist voorafgaande authenticatie en er is geen publieke Proof-of-Concept-code (PoC) of exploit beschikbaar. Maar deze kwetsbaarheid stelt een kwaadwillende wel in staat om volledige controle over het kwetsbare systeem te krijgen.

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/august-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-0059	6.0 MEDIUM
CVE-2025-23194	5.3 MEDIUM
CVE-2025-27429	8.7 HIGH

CVE-2025-31331	4.3 MEDIUM
CVE-2025-42934	5.3 MEDIUM
CVE-2025-42935	1.8 LOW
CVE-2025-42936	5.3 MEDIUM
CVE-2025-42941	4.8 MEDIUM
CVE-2025-42942	5.3 MEDIUM
CVE-2025-42943	4.8 MEDIUM
CVE-2025-42946	4.8 MEDIUM
CVE-2025-42948	5.3 MEDIUM
CVE-2025-42949	5.1 MEDIUM
CVE-2025-42950	8.7 HIGH
CVE-2025-42951	8.7 HIGH
CVE-2025-42955	5.1 MEDIUM
CVE-2025-42957	8.7 HIGH
CVE-2025-42975	5.3 MEDIUM
CVE-2025-42976	5.3 MEDIUM
CVE-2025-42945	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-1022	Use of Web Link to Untrusted Target with window.opener Access
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-266	Incorrect Privilege Assignment

CWE-532	Insertion of Sensitive Information into Log File
CWE-250	Execution with Unnecessary Privileges
CWE-125	Out-of-bounds Read
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-863	Incorrect Authorization
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
SAP S/4HANA (Private Cloud)
SAP Landscape Transformation (Analysis Platform)
SAP Business One (SLD)
SAP NetWeaver Application Server ABAP (BIC Document)
NetWeaver Application Server ABAP
SAP S/4HANA (Bank Communication Management)
SAP NetWeaver Application Server ABAP
SAP NetWeaver Application Server for ABAP
NetWeaver Application Server for ABAP
SAP NetWeaver Enterprise Portal (OBN component)

ABAP Platform
SAP GUI for Windows

Disclaimer