Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0356

Kwetsbaarheden verholpen in SAP-producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-11-2025

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 verschillende producten, waaronder SAP NetWeaver, SAP Business Connector, SAP HANA, en SAP S/4HANA.

Duiding

De kwetsbaarheden omvatten onder andere deserialisatie, code-injectie, onvoldoende validatie, en informatie openbaarmaking. Deze kwetsbaarheden kunnen worden misbruikt door aanvallers om ongeautoriseerde toegang te verkrijgen, schadelijke code uit te voeren, of gevoelige informatie te lekken. De impact varieert van compromittering van vertrouwelijkheid en integriteit tot volledige systeemcompromittering, afhankelijk van de specifieke kwetsbaarheid en de context van gebruik.

De ernstigste kwetsbaarheid heeft kenmerk CVE-2025-42944 toegewezen gekregen en bevindt zich in Netweaver. Een kwaadwillende op afstand kan de kwetsbaarheid zonder voorafgaande authenticatie misbruiken om willekeurige code uit te voeren in de context van de Netweaver service.

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/november-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-42890	9.3 CRITICAL
CVE-2025-42944	9.3 CRITICAL
CVE-2025-42887	8.7 HIGH
CVE-2025-42940	6.9 MEDIUM
CVE-2025-42895	4.6 MEDIUM

CVE-2025-42892	8.5 HIGH
CVE-2025-42894	8.5 HIGH
CVE-2025-42884	6.9 MEDIUM
CVE-2025-42924	5.3 MEDIUM
CVE-2025-42893	5.3 MEDIUM
CVE-2025-42886	5.3 MEDIUM
CVE-2025-42885	6.9 MEDIUM
CVE-2025-42888	4.6 MEDIUM
CVE-2025-42889	5.3 MEDIUM
CVE-2025-42919	6.9 MEDIUM
CVE-2025-42897	6.9 MEDIUM
CVE-2025-42899	5.3 MEDIUM
CVE-2025-42882	5.3 MEDIUM
CVE-2025-42883	5.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
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-316	Cleartext Storage of Sensitive Information in Memory
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-502	Deserialization of Untrusted Data
CWE-522	Insufficiently Protected Credentials
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-787	Out-of-bounds Write
CWE-798	Use of Hard-coded Credentials
CWE-862	Missing Authorization
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

SAP
Business One
GUI for Windows
HANA
HANA JDBC Client
NetWeaver Application Server Java
NetWeaver Application Server for ABAP
NetWeaver Enterprise Portal
Netweaver
S4CORE
SAP Netweaver (RMI-P4)
SQL Anywhere Monitor

Solution Manager

Disclaimer