Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0219

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 09-07-2025

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 S/4HANA, SAP SCM, en SAP NetWeaver.

Duiding

De kwetsbaarheden omvatten onder andere remote code execution, code injectie, en insecure deserialization, die door aanvallers met gebruikersprivileges kunnen worden misbruikt om schadelijke code te creëren of uit te voeren. Dit kan leiden tot ernstige bedreigingen voor de vertrouwelijkheid, integriteit en beschikbaarheid van de getroffen systemen. Specifieke kwetsbaarheden zoals een replay-aanval en privilege-escalatie zijn ook geïdentificeerd, wat de noodzaak benadrukt voor strikte autorisatiecontroles en monitoring van de systemen. De impact varieert van ongeautoriseerde toegang tot gegevens tot volledige systeemcompromittering.

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/july-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-42967	8.6 HIGH
CVE-2025-42980	8.6 HIGH
CVE-2025-42964	8.6 HIGH
CVE-2025-42966	8.6 HIGH
CVE-2025-42963	8.6 HIGH
CVE-2025-42959	9.2 CRITICAL
CVE-2025-42953	5.3 MEDIUM

CVE-2024-53677	9.5 CRITICAL
CVE-2025-42952	7.1 HIGH
CVE-2025-43001	4.6 MEDIUM
CVE-2025-42981	5.3 MEDIUM
CVE-2025-42969	5.3 MEDIUM
CVE-2025-42962	5.3 MEDIUM
CVE-2025-42985	5.3 MEDIUM
CVE-2025-42970	4.6 MEDIUM
CVE-2025-42979	2.0 LOW
CVE-2025-42973	5.1 MEDIUM
CVE-2025-42968	5.3 MEDIUM
CVE-2025-42961	5.1 MEDIUM
CVE-2025-42960	5.3 MEDIUM
CVE-2025-42986	5.3 MEDIUM
CVE-2025-42974	5.3 MEDIUM
CVE-2025-31326	5.1 MEDIUM
CVE-2025-42965	5.1 MEDIUM
CVE-2025-42971	4.6 MEDIUM
CVE-2025-42978	6.3 MEDIUM
CVE-2025-42954	5.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-940	Improper Verification of Source of a Communication Channel
CWE-308	Use of Single-factor Authentication
CWE-922	Insecure Storage of Sensitive Information
CWE-266	Incorrect Privilege Assignment
CWE-80	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-552	Files or Directories Accessible to External Parties
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-862	Missing Authorization
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-502	Deserialization of Untrusted Data
CWE-918	Server-Side Request Forgery (SSRF)
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

SAP
SAP S/4HANA and SAP SCM (Characteristic Propagation)

S4HANA, SCM
Business Warehouse, BW-4HANA BEx Tools
SAP Business Warehouse and SAP BW/4HANA BEx Tools
s/ 4hana
scm
NetWeaver Enterprise Portal Federated Portal Network
NetWeaver Enterprise Portal Administration
SAP NetWeaver (XML Data Archiving Service)
SAP NetWeaver Application Server for Java (Log Viewer)
NetWeaver ABAP Server, ABAP Platform
SAP BusinessObjects Business Intelligence Platform (Web Intelligence)
NetWeaver Business Warehouse
Business Warehouse and Plug-In Basis
SAPCAR
SAP Business Warehouse (Business Explorer Web 3.5 loading animation)
BusinessObjects Content Administrator workbench
businessobjects_content_administrator_workbench

SAP BusinessObjects Content Administrator workbench
SAP GUI for Windows
SAP Data Services (DQ Report)
SAP NetWeaver and ABAP Platform (SDCCN)
SAP NetWeaver Application Server Java

Disclaimer