Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0149

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-05-2025

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 diverse SAP producten, zoals NetWeaver, NetWeaver Visual Composer, SAP GUI, pcde, Business Objects, HANA en andere componenten.

Duiding

De kwetsbaarheden omvatten onder andere een onbeperkte bestandsuploadfout die ongeauthenticeerde gebruikers in staat stelt om kwaadaardige bestanden te uploaden, wat kan leiden tot uitvoer van willekeurige code. Daarnaast zijn er kwetsbaarheden gerapporteerd die voortkomen uit het ontbreken van noodzakelijke autorisatiecontroles, wat kan resulteren in ongeoorloofde toegang tot gevoelige gegevens en privilege-escalatie.

SAP brengt de kwetsbaarheid met kenmerk CVE-2025-31324 opnieuw onder de aandacht. Deze kwetsbaarheid bevindt zich in de NetWeaver Visual Component en is in de maandelijkse update van april verholpen. Deze kwetsbaarheid is echter als ZeroDay actief misbruikt.

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/may-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-42999	9.1 CRITICAL
CVE-2025-30018	8.6 HIGH
CVE-2025-43010	8.3 HIGH
CVE-2025-43000	7.9 HIGH
CVE-2025-43011	7.7 HIGH
CVE-2024-39592	7.7 HIGH

CVE-2025-42997	6.6 MEDIUM
CVE-2025-43003	6.4 MEDIUM
CVE-2025-43009	6.3 MEDIUM
CVE-2025-43007	6.3 MEDIUM
CVE-2025-31329	6.2 MEDIUM
CVE-2025-43006	6.1 MEDIUM
CVE-2025-43008	5.8 MEDIUM
CVE-2025-43004	5.3 MEDIUM
CVE-2025-26662	4.4 MEDIUM
CVE-2025-43002	4.3 MEDIUM
CVE-2025-43005	4.3 MEDIUM
CVE-2025-31324	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-141	Improper Neutralization of Parameter/Argument Delimiters
CWE-749	Exposed Dangerous Method or Function
CWE-472	External Control of Assumed-Immutable Web Parameter
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-256	Plaintext Storage of a Password
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-285	Improper Authorization
CWE-862	Missing Authorization
CWE-94	Improper Control of Generation of Code ('Code Injection')

CWE-502	Deserialization of Untrusted Data
CWE-611	Improper Restriction of XML External Entity Reference
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

SAP
Netweaver
SAP Business Objects Business Intelligence Platform (PMW)
SAP Data Services Management Console
NetWeaver
SAP Digital Manufacturing (Production Operator Dashboard)
SAP GUI for Windows
SAP Gateway Client
SAP Landscape Transformation (PCL Basis)
SAP NetWeaver (Visual Composer development server)
SAP NetWeaver Application Server ABAP and ABAP Platform
SAP S/4HANA (Private Cloud & On-Premise)
SAP S/4HANA Cloud Private Edition or on Premise (SCM Master Data Layer (MDL))

SAP S/4HANA HCM Portugal and SAP ERP HCM Portugal
SAP S4/HANA (OData meta-data property)
SAP Service Parts Management (SPM)
SAP Software
SAP Supplier Relationship Management (Live Auction Cockpit)
SAP Supplier Relationship Management (Master Data Management Catalog)
netweaver
pdce
sap
s4coreop
sap_pdce

Disclaimer