Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0045

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-02-2025

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 onder andere SAP NetWeaver, BusinessObjects Business Intelligence platform, Enterprise Project Connection en Commerce.

Duiding

De kwetsbaarheden in SAP NetWeaver omvatten een gebrek aan toegangscontrole, wat ongeauthenticeerde aanvallers in staat stelt om toegang te krijgen tot gevoelige serverinstellingen en gegevens. Daarnaast zijn er Cross-Site Scripting kwetsbaarheden in SAP producten die de vertrouwelijkheid van gegevens ernstig kunnen aantasten. De kwetsbaarheden kunnen worden misbruikt door aanvallers om ongeautoriseerde toegang te verkrijgen tot gevoelige informatie, wat kan leiden tot datalekken en andere beveiligingsincidenten.

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/february-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-24527	5.3 MEDIUM
CVE-2024-22126	8.8 HIGH
CVE-2024-38819	6.9 MEDIUM
CVE-2024-38820	2.3 LOW
CVE-2024-38828	6.9 MEDIUM
CVE-2024-45216	9.3 CRITICAL
CVE-2024-45217	5.1 MEDIUM
CVE-2025-0054	5.1 MEDIUM

CVE-2025-0064	5.1 MEDIUM
CVE-2025-23187	6.9 MEDIUM
CVE-2025-23189	5.3 MEDIUM
CVE-2025-23190	5.3 MEDIUM
CVE-2025-23191	2.3 LOW
CVE-2025-23193	6.9 MEDIUM
CVE-2025-24867	5.3 MEDIUM
CVE-2025-24868	5.3 MEDIUM
CVE-2025-24869	5.3 MEDIUM
CVE-2025-24870	4.6 MEDIUM
CVE-2025-24872	5.3 MEDIUM
CVE-2025-24874	2.3 LOW
CVE-2025-24875	5.3 MEDIUM
CVE-2025-24876	5.3 MEDIUM
CVE-2025-25241	5.3 MEDIUM
CVE-2025-25243	6.9 MEDIUM

CWE's

CWE	Beschrijving
CWE-921	Storage of Sensitive Data in a Mechanism without Access Control
CWE-1021	Improper Restriction of Rendered UI Layers or Frames
CWE-1188	Initialization of a Resource with an Insecure Default
CWE-178	Improper Handling of Case Sensitivity
CWE-732	Incorrect Permission Assignment for Critical Resource

CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-644	Improper Neutralization of HTTP Headers for Scripting Syntax
CWE-204	Observable Response Discrepancy
CWE-404	Improper Resource Shutdown or Release
CWE-306	Missing Authentication for Critical Function
CWE-862	Missing Authorization
CWE-352	Cross-Site Request Forgery (CSRF)
CWE-284	Improper Access Control
CWE-863	Incorrect Authorization
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-287	Improper Authentication
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

sap
supplier_relationship_management
netweaver
netweaver_server_abap
netweaver_java_application_server
netweaver_as_java
netweaver_application_server_java
netweaver_as_java_for_deploy_service
abap_platform
commerce_backoffice

commerce

Disclaimer