Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0007

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-01-2025

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 SAP, NetWeaver en ABAP.

Duiding

De kwetsbaarheden in SAP NetWeaver Application Server voor ABAP en ABAP Platform omvatten onjuiste authenticatiecontroles en zwakke toegangscontroles, die door geauthenticeerde aanvallers kunnen worden misbruikt om hun privileges te escaleren en ongeautoriseerde toegang tot gevoelige gegevens te verkrijgen. Dit kan leiden tot compromittering van de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem. Daarnaast zijn er kwetsbaarheden gerapporteerd die SQL-injectie en cross-site scripting mogelijk maken, wat verdere risico's met zich meebrengt.

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/january-2025.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-0070	9.9 CRITICAL
CVE-2025-0066	9.9 CRITICAL
CVE-2025-0063	8.8 HIGH
CVE-2025-0061	8.7 HIGH
CVE-2025-0069	7.8 HIGH
CVE-2025-0058	6.5 MEDIUM
CVE-2025-0067	6.3 MEDIUM
CVE-2025-0055	6.0 MEDIUM

CVE-2025-0056	**6.0 MEDIUM**
CVE-2025-0059	**6.0 MEDIUM**
CVE-2025-0053	**5.3 MEDIUM**
CVE-2025-0057	**4.8 MEDIUM**
CVE-2025-0068	**4.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-497	Exposure of Sensitive System Information to an Unauthorized Control Sphere
CWE-732	Incorrect Permission Assignment for Critical Resource
CWE-427	Uncontrolled Search Path Element
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-862	Missing Authorization
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-209	Generation of Error Message Containing Sensitive Information
CWE-287	Improper Authentication

Getroffen producten

sap
sap
sap_se
sap_business_workflow_and_sap_flexible_workflow

sap_businessobjects_business_intelligence_platform
sap_gui_for_java
sap_gui_for_windows
sap_netweaver_application_server_abap
sap_netweaver_application_server_abap__applications_based_on_sap_gui_for_html_
sap_netweaver_application_server_for_abap_and_abap_platform
sap_netweaver_application_server_java
sap_netweaver_as_abap_and_abap_platform
sap_netweaver_as_for_abap_and_abap_platform__internet_communication_framework_
sap_netweaver_as_java__user_admin_application_
sapsetup

Disclaimer