



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

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.