



NCSC-2024-0378

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 19-09-2024

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 diverse producten, zoals SAP, Business Warehouse, NetWeaver, HANA, Business Objects en Commerce.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Cross-Site Scripting (XSS)
- Omzeilen van authenticatie
- Omzeilen van beveiligingsmaatregel
- Uitvoer van willekeurige code (gebruikersrechten)
- Toegang tot gevoelige gegevens

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/september-2024.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2013-3587	5.9 MEDIUM
➤ CVE-2024-41728	2.7 LOW
➤ CVE-2024-41729	4.3 MEDIUM
➤ CVE-2024-42371	5.4 MEDIUM
➤ CVE-2024-42378	6.1 MEDIUM
➤ CVE-2024-42380	5.4 MEDIUM

> CVE-2024-44112	4.3 MEDIUM
> CVE-2024-44113	4.3 MEDIUM
> CVE-2024-44114	2.7 LOW
> CVE-2024-44115	5.4 MEDIUM
> CVE-2024-44116	5.4 MEDIUM
> CVE-2024-44117	5.4 MEDIUM
> CVE-2024-44120	4.7 MEDIUM
> CVE-2024-44121	4.3 MEDIUM
> CVE-2024-45279	6.1 MEDIUM
> CVE-2024-45280	4.8 MEDIUM
> CVE-2024-45281	5.8 MEDIUM
> CVE-2024-45283	6.0 MEDIUM
> CVE-2024-45284	2.7 LOW
> CVE-2024-45285	5.4 MEDIUM
> CVE-2024-45286	6.5 MEDIUM

CWE's

CWE	Beschrijving
> CVE-359	Exposure of Private Personal Information to an Unauthorized Actor
> CVE-213	Exposure of Sensitive Information Due to Incompatible Policies
> CVE-426	Untrusted Search Path
> CVE-256	Plaintext Storage of a Password
> CVE-325	Missing Cryptographic Step
> CVE-862	Missing Authorization

➤ CWE-863	Incorrect Authorization
➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

sap
business_warehouse
businessobjects_business_intelligence_platform
commerce_cloud
netweaver_application_server_abap
netweaver_application_server_for_abap
netweaver_as_for_java
netweaver_as_java
netweaver_bw
netweaver_enterprise_portal
oil_\%\ _gas
oil_gas
production_and_revenue_accounting
sap
student_life_cycle_management
sap_se
sap_business_warehouse__bex_analyzer_
sap_businessobjects_business_intelligence_platform
sap_for_oil__gas
sap_netweaver_application_server_for_abap__crm_blueprint_application_builder_panel_

sap_netweaver_application_server_for_abap_and_abap_platform

sap_netweaver_as_for_java__destination_service_

sap_netweaver_as_java__logon_application_

sap_netweaver_bw__bex_analyzer_

sap_netweaver_enterprise_portal

sap_production_and_revenue_accounting__tobin_interface_

sap_s_4_hana__statutory_reports_

sap_s_4hana_eprocurement

sap_student_life_cycle_management__slcm_

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.