



NCSC-2024-0333

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2024

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 als SAP Business Objects, SAP HANA, Netweaver en Document Builder.

Duiding

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

- Server Side Request Forgery (SSRF)
- Cross-Site Scripting (XSS)
- Omzeilen van authenticatie
- Omzeilen van beveiligingsmaatregel
- Manipulatie van gegevens
- Toegang tot gevoelige gegevens

Oplossingen

SAP heeft updates uitgebracht om de kwetsbaarheden te verhelpen in de kwetsbare producten. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2022-0778	
➤ CVE-2023-0215	
➤ CVE-2023-0286	
➤ CVE-2023-30533	
➤ CVE-2024-28166	4.3 MEDIUM
➤ CVE-2024-29415	

> CVE-2024-33003	7.4 HIGH
> CVE-2024-33005	6.3 MEDIUM
> CVE-2024-39591	4.3 MEDIUM
> CVE-2024-41730	9.8 CRITICAL
> CVE-2024-41731	4.3 MEDIUM
> CVE-2024-41732	4.7 MEDIUM
> CVE-2024-41733	5.3 MEDIUM
> CVE-2024-41734	4.3 MEDIUM
> CVE-2024-41735	5.4 MEDIUM
> CVE-2024-41736	4.3 MEDIUM
> CVE-2024-41737	5.0 MEDIUM
> CVE-2024-42373	
> CVE-2024-42374	8.2 HIGH
> CVE-2024-42375	4.3 MEDIUM
> CVE-2024-42376	6.5 MEDIUM

CWE's

CWE	Beschrijving
> CVE-20	Improper Input Validation
> CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
> CVE-284	Improper Access Control
> CVE-416	Use After Free
> CVE-434	Unrestricted Upload of File with Dangerous Type
> CVE-704	Incorrect Type Conversion or Cast

➤ CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
➤ CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
➤ CWE-862	Missing Authorization
➤ CWE-91	XML Injection (aka Blind XPath Injection)
➤ CWE-918	Server-Side Request Forgery (SSRF)

Getroffen producten

sap_se
sap_bex_web_java_runtime_export_web_service
sap_businessobjects_business_intelligence_platform
sap_commerce_backoffice
sap_commerce_cloud
sap_commerce
sap_crm_abap__insights_management_
sap_document_builder
sap_netweaver_application_server__abap_and_java__sap_web_dispatcher_and_sap_content_server
sap_netweaver_application_server_abap_and_abap_platform
sap_netweaver_application_server_abap
sap_permit_to_work
sap_shared_service_framework
sap_student_life_cycle_management__slcm_
sap
businessobjects_business_intelligence_platform
commerce_backoffice

document_builder
sap
student_life_cycle_management

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.