



NCSC-2024-0228

Kwetsbaarheden verholpen in SAP producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 17-05-2024

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 NetWeaver, Business Objects, HANA en SAP GUI.

Duiding

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

- Cross-Site-Scripting (XSS)
- Denial-of-Service (DoS)
- Manipulatie van gegevens
- Omzeilen van authenticatie
- (Remote) code execution (Gebruikersrechten)
- SQL Injection
- Toegang tot gevoelige gegevens

Oplossingen

SAP heeft updates beschikbaar gesteld om de kwetsbaarheden te verhelpen in de getroffen producten. Zie bijgevoegde referenties voor meer informatie:

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

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2022-36364	
➤ CVE-2024-4138	
➤ CVE-2024-4139	
➤ CVE-2024-28165	8.1 HIGH

> CVE-2024-32730
> CVE-2024-32731
> CVE-2024-32733
> CVE-2024-33000
> CVE-2024-33002
> CVE-2024-33004
> CVE-2024-33006
> CVE-2024-33007
> CVE-2024-33008
> CVE-2024-33009
> CVE-2024-34687

CWE's

CWE	Beschrijving
> CVE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer
> CVE-434	Unrestricted Upload of File with Dangerous Type
> CVE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CVE-862	Missing Authorization
> CVE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CVE-922	Insecure Storage of Sensitive Information

Getroffen producten

sap
bank_account_management
businessobjects_business_intelligence_platform_webservices_
businessobjects_business_intelligence_platform
global_label_management
my_travel_requests
netweaver_application_server_abap_and_abap_platform
netweaver_application_server_abap
replication_server
ui5

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.