Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0228

Kwetsbaarheden verholpen in SAP producten

2024-05-17 Revisie 0

Toegestande verspreiding: 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.firs t.org/tlp). Ontvangers mogen de informatie delen met collega's van andere organisaties, informatiefora of personen werkzaam in netwerkbeveiliging, informatiebeveiliging of de VI-gemeenschap in de bredere zin. Het is niet de bedoeling dat u de informatie publiek maakt.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

SAP heeft kwetsbaarheden verholpen in diverse producten, zoals NetWeaver, Business Objects, HANA en SAP GUI.

Interpretaties

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