



## Advisory NCSC-2024-0378

# Kwetsbaarheden verholpen in SAP producten

2024-09-19 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.first.org/tlp](http://www.first.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](mailto:info@ncsc.nl)

## Feiten

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

---

## Interpretaties

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>