Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2024-0229

Kwetsbaarheid verholpen in QlikSense Enterprise

2024-05-22 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

Er is een kwetsbaarheid verholpen in QlikSense Enterprise.

Interpretaties

Een kwaadwillende kan de kwetsbaarheid misbruiken om zichzelf verhoogde rechten toe te kennen en zo mogelijk willekeurige code uitvoeren op het systeem waarop QlikSense is geïnstalleerd.

Voor succesvol misbruik moet de kwaadwillende voorafgaande authenticatie hebben op de kwetsbare applicatie.

Oplossingen

QlikSense heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie:

https://community.qlik.com/t5/Support-Updates/Qlik-Sense-Enterprise-for-Windows-New-Security-Patches-Available/ba-p/2452521

Referenties

- https://community.qlik.com/t5/Official-Support-Articles/High-Severity-Security-fixes-for-Qlik-Sense-Enterprise-for/ta-p/2452509
- https://community.qlik.com/t5/Support-Updates/Qlik-Sense-Enterprise-for-Windows-New-Security-Patches-Available/ba-p/2452521