Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2025-0064

Kwetsbaarheden verholpen in IBM Cognos Controller

2025-02-21 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

IBM heeft kwetsbaarheden verholpen in IBM Cognos Controller (Versies 11.0.0 tot 11.0.1 FP3 en 11.1.0).

Interpretaties

De kwetsbaarheden stellen een kwaadwillende in staat om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Denial-of-Service (DoS)
- Cross-Site-Scripting (XSS)
- Omzeilen van een beveiligingsmaatregel
- Manipulatie van gegevens
- Verkrijgen van verhoogde rechten
- Uitvoer van willekeurige code (Gebruikersrechten)
- Toegang tot gevoelige informatie

De kwetsbaarheden bevinden zich zowel in de Cognos Controller-Applicatie zelf, als in onderliggende producten, zoals Java, Websphere Liberty, Apache Ant en diverse Open Source componenten, welke met Cognos Controller worden meegeleverd.

Oplossingen

IBM heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://www.ibm.com/support/pages/node/7183597