Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0269

Kwetsbaarheden verholpen in IBM Cognos Command Center

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 27-08-2025

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

IBM heeft kwetsbaarheden verholpen in IBM Cognos Command Center (Versies 10.2.4.1 en 10.2.5).

Duiding

De kwetsbaarheden in IBM Cognos Command Center stellen kwaadwillenden in staat om klikacties van slachtoffers te kapen door hen te misleiden naar een kwaadaardige website te navigeren. Dit kan leiden tot verdere aanvallen die de integriteit van gebruikersinteracties in gevaar brengen. Daarnaast kunnen lokale gebruikers willekeurige code uitvoeren door een onveilige implementatie van de BinaryFormatter-functie. Ook is er een open redirect-mechanisme aanwezig dat kan worden misbruikt voor phishing-aanvallen, wat kan resulteren in het compromitteren van gevoelige informatie. Het is niet ondenkbaar, dat het misbruiken in keten een kwaadwillende in staat kan stellen om zonder voorafgaande authenticatie willekeurige code uit te voeren met rechten van het slachtoffer en toegang te krijgen tot gevoelige gegevens.

Oplossingen

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

Referenties

- https://www.ibm.com/support/pages/node/7242159

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-1494	6.1 MEDIUM
CVE-2025-1994	7.8 HIGH
CVE-2025-2697	7.4 HIGH
CVE-2025-2900	7.5 HIGH
CVE-2025-4447	7.0 HIGH

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-242	Use of Inherently Dangerous Function
CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
CWE-787	Out-of-bounds Write
CWE-1021	Improper Restriction of Rendered UI Layers or Frames

Getroffen producten

IBM
Cognos Command Center

Disclaimer