Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0064

Kwetsbaarheden verholpen in IBM Cognos Controller

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 21-02-2025

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 Controller (Versies 11.0.0 tot 11.0.1 FP3 en 11.1.0).

Duiding

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

Kwetsbaarheden

CVE	CVSS Score
› CVE-2020-11979	7.5 HIGH
› CVE-2021-36373	
› CVE-2021-36374	

CVE-2022-4244	7.5 HIGH
CVE-2022-4245	4.3 MEDIUM
CVE-2023-47160	8.2 HIGH
CVE-2023-50314	6.3 MEDIUM
CVE-2024-21131	
CVE-2024-21144	
CVE-2024-21145	
CVE-2024-27267	8.2 HIGH
CVE-2024-28776	5.4 MEDIUM
CVE-2024-28777	8.8 HIGH
CVE-2024-28780	5.9 MEDIUM
CVE-2024-38999	8.9 HIGH
CVE-2024-45081	6.5 MEDIUM
CVE-2024-45084	8.0 HIGH
CVE-2024-52902	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-399	CWE-399
CWE-379	Creation of Temporary File in Directory with Insecure Permissions
CWE-300	Channel Accessible by Non-Endpoint
CWE-798	Use of Hard-coded Credentials
CWE-284	Improper Access Control

CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-295	Improper Certificate Validation
CWE-91	XML Injection (aka Blind XPath Injection)
CWE-94	Improper Control of Generation of Code ('Code Injection')
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-502	Deserialization of Untrusted Data
CWE-377	Insecure Temporary File
CWE-863	Incorrect Authorization
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-611	Improper Restriction of XML External Entity Reference
CWE-787	Out-of-bounds Write
CWE-20	Improper Input Validation
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

ibm
cognos_controller

Disclaimer