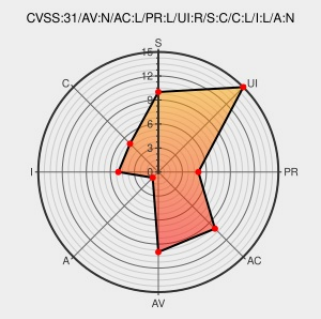
CVE-2021-38946

Published on: Not Yet Published

Last Modified on: 10/18/2022 08:34:00 PM UTC

CVE-2021-38946

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Cognos Analytics from Ibm contain the following vulnerability:

IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 211240.

CVE-2021-38946 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **IBM** - **Cognos Analytics** version **11.2.0**

Affected Vendor/Software: **IBM** - **Cognos Analytics** version **11.1.7**

Affected Vendor/Software: **IBM** - **Cognos Analytics** version **11.2.1**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Bulletin: IBM Cognos Analytics has addressed multiple vulnerabilities	www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6570957
March 2022 IBM Cognos Analytics Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20220602-0003/
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-cognos-cve202138946-xss (211240)

There are currently no QIDs associated with this CVE

Exploit/POC from Github

IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulnerability allows user…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Cognos Analytics	11.1.7	-	All	All
Application	Ibm	Cognos Analytics	11.2.0	All	All	All
Application	Ibm	Cognos Analytics	11.2.1	All	All	All
Application	Netapp	Oncommand Insight	-	All	All	All

cpe:2.3:a:ibm:cognos_analytics:11.1.7:-:*:*:*:*:*:*:

cpe:2.3:a:ibm:cognos_analytics:11.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:cognos_analytics:11.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:oncommand_insight:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-38946 : #IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulne… twitter.com/i/web/status/1…	2022-04-22 16:39:09
@threatmeter	CVE-2021-38946 IBM Cognos Analytics 11.1.7, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulnerab… twitter.com/i/web/status/1…	2022-04-23 07:09:49

/r/netcve	CVE-2021-38946	2022-04-22 17:38:28

← Previous ID

Next ID→