

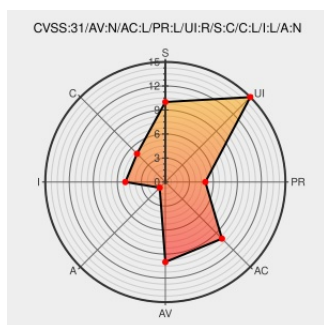


CVE-2021-38946

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)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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

[← Previous ID](#)[Next ID→](#)© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)