



CVE-2021-38945

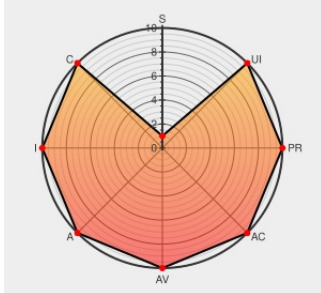
Published on: Not Yet Published

Last Modified on: 10/28/2022 10:32:00 PM UTC

CVE-2021-38945

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Cognos Analytics](#) from [Ibm](#) contain the following vulnerability:

IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 could allow a remote attacker to upload arbitrary files, caused by improper content validation. IBM X-Force ID: 211238.

CVE-2021-38945 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **CRITICAL** 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: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

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/6597241
June 2022 IBM Cognos Analytics Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20220729-0002/
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF ibm-cognos-cve202138945-file-upload (211238)

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Cognos Analytics	All	All	All	All
Application	Ibm	Cognos Analytics	11.1.7	-	All	All
Application	Ibm	Cognos Analytics	11.1.7	fixpack1	All	All
Application	Ibm	Cognos Analytics	11.1.7	fixpack2	All	All
Application	Ibm	Cognos Analytics	11.1.7	fixpack3	All	All
Application	Ibm	Cognos Analytics	11.1.7	fixpack4	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:*.:.:.:.:.:.:
```

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

```
cpe:2.3:a:ibm:cognos_analytics:11.1.7:fixpack1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:cognos_analytics:11.1.7:fixpack2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:cognos_analytics:11.1.7:fixpack3:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:cognos_analytics:11.1.7:fixpack4:*:*:*:*:*:
```

```
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-2021-38945 : #IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 could allow a remote attacker to upload arbitrary... twitter.com/i/web/status/1...	2022-06-24 15:40:24
/r/netcve	CVE-2021-38945	2022-06-24 16:38:28

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.report and Source URL Uptime Status status.cve.report