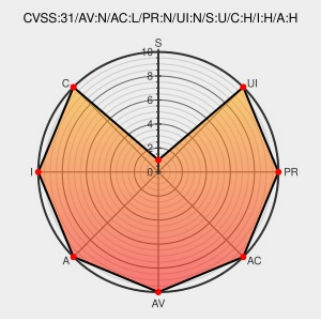
CVE-2020-4879

Published on: 01/21/2022 12:00:00 AM UTC

Last Modified on: 01/27/2022 02:26:00 PM UTC

CVE-2020-4879

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



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

IBM Cognos Controller 10.4.0, 10.4.1, and 10.4.2 could allow a remote attacker to bypass security restrictions, caused by improper validation of authentication cookies. IBM X-Force ID: 190847.

CVE-2020-4879 has been assigned by psirt@us.ibm.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **IBM** - **Cognos Controller** version **10.4.0**

Affected Vendor/Software: **IBM** - **Cognos Controller** version **10.4.1**

Affected Vendor/Software: **IBM** - **Cognos Controller** version **10.4.2**

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 Controller has addressed multiple vulnerabilities	www.ibm.com text/html	CONFIRM www.ibm.com/support/pages/node/6509856
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF ibm-cognos-cve20204879-priv-escalation (190847)

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 Controller	10.4.0	All	All	All
Application	Ibm	Cognos Controller	10.4.1	All	All	All
Application	Ibm	Cognos Controller	10.4.2	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:a:ibm:cognos_controller:10.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:cognos_controller:10.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:ibm:cognos_controller:10.4.2:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-4879 : #IBM Cognos Controller 10.4.0, 10.4.1, and 10.4.2 could allow a remote attacker to bypass security… twitter.com/i/web/status/1…	2022-01-21 17:25:21
/r/netcve	CVE-2020-4879	2022-01-21 18:38:57

← Previous ID

Next ID→

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