

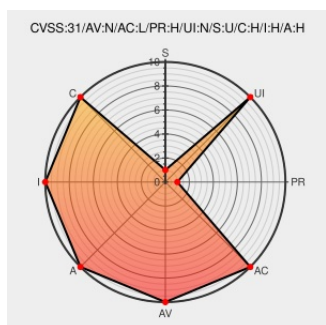


CVE-2020-4685

Published on: 11/11/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-4685

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

Certain versions of **Cognos Controller** from **IBM** contain the following vulnerability:

A low level user of IBM Cognos Controller 10.3.0, 10.3.1, 10.4.0, 10.4.1, and 10.4.2 who has Administration rights to the server where the application is installed, can escalate their privilege from Low level to Super Admin and gain access to Create/Update/Delete any level of user in Cognos Controller. IBM X-Force ID: 186625.

CVE-2020-4685 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [IBM](#) - **Cognos Controller** version **10.3.1**

Affected Vendor/Software: [IBM](#) - **Cognos Controller** version **10.3.0**

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: **7.2 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

impact

impact

impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description	Tags	Link
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-cognos-cve20204685-priv-escalation (186625)
Security Bulletin: IBM Cognos Controller is vulnerable to privilege escalation (CVE-2020-4685)	Patch Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6339995

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	10.3.0	All	All	All
Application	Ibm	Cognos Controller	10.3.1	All	All	All
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
Application	Ibm	Cognos Controller	10.3.0	All	All	All
Application	Ibm	Cognos Controller	10.3.1	All	All	All
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

```
cpe:2.3:a:ibm:cognos_controller:10.3.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:cognos_controller:10.3.1:*:*:*:*:*:*:
```

```
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:a:ibm:cognos_controller:10.3.0:*:*:*:*:*:
```

```
one:2 3:2 ihm:cognos controller:10 3 1:*. *. *. *. *. *. *
```

cpe:2.3:a:ibm:cognos_controller:10.0.1:*:*:*:*:*:
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:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)