

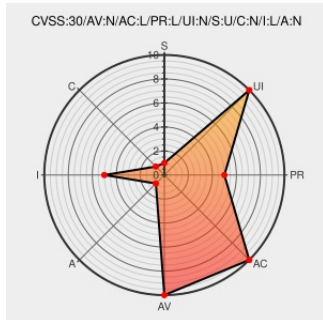


CVE-2017-1766

Published on: 03/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:37 PM UTC

CVE-2017-1766

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

Certain versions of [Business Process Manager](#) from [Ibm](#) contain the following vulnerability:

Due to incorrect authorization in IBM Business Process Manager 8.6 an attacker can claim and work on ad hoc tasks he is not assigned to. IBM X-Force ID: 136151.

CVE-2017-1766 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [IBM](#) - **Business Process Manager** version 8.6

Affected Vendor/Software: [IBM](#) - **Business Process Manager** version 8.6.0.CF201712

CVSS3 Score: **4.3 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
IBM X-Force ID: 136151	X-Force	X-Force

IBM X-Force Exchange

VDB Entry

Vendor Advisory

exchange.xforce.ibmcloud.com

text/html

MISC

exchange.xforce.ibmcloud.com/vulnerabilities/136151

Security Bulletin: Incorrect authorization for task assignment of ad hoc tasks in views shipped with IBM Business Process Manager (CVE-2017-1766)

Patch

Vendor Advisory

www.ibm.com

text/html

CONFIRM

www.ibm.com/support/docview.wss?uid=swg22011866

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	Business Process Manager	8.5.5.0	All	All	All
Application	IBM	Business Process Manager	8.5.5.0	All	All	All
Application	IBM	Business Process Manager	8.5.5.0	All	All	All
Application	IBM	Business Process Manager	8.5.6.0	All	All	All
Application	IBM	Business Process Manager	8.5.6.0	All	All	All
Application	IBM	Business Process Manager	8.5.6.0	All	All	All
Application	IBM	Business Process Manager	8.5.6.0	cf2	All	All
Application	IBM	Business Process Manager	8.5.6.0	cf2	All	All
Application	IBM	Business Process Manager	8.5.6.0	cf2	All	All
Application	IBM	Business Process Manager	8.5.6.1	All	All	All
Application	IBM	Business Process Manager	8.5.6.1	All	All	All
Application	IBM	Business Process Manager	8.5.6.1	All	All	All
Application	IBM	Business Process Manager	8.5.6.2	All	All	All
Application	IBM	Business Process Manager	8.5.6.2	All	All	All
Application	IBM	Business Process Manager	8.5.6.2	All	All	All
Application	IBM	Business Process Manager	8.5.7.0	All	All	All
Application	IBM	Business Process Manager	8.5.7.0	All	All	All
Application	IBM	Business Process Manager	8.5.7.0	All	All	All
Application	IBM	Business Process Manager	8.5.7.0	cf201606	All	All
Application	IBM	Business Process Manager	8.5.7.0	cf201606	All	All
Application	IBM	Business Process Manager	8.5.7.0	cf201606	All	All
Application	IBM	Business Process Manager	8.5.7.0	cf201609	All	All
Application	IBM	Business Process Manager	8.5.7.0	cf201609	All	All

[illegible]

Application	Ibm	Business Process Manager	8.5.7.0	cf201609	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201612	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201612	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201612	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201703	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201703	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201703	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201706	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201706	All	All
Application	Ibm	Business Process Manager	8.5.7.0	cf201706	All	All
Application	Ibm	Business Process Manager	8.6.0.0	All	All	All
Application	Ibm	Business Process Manager	8.6.0.0	cf201712	All	All
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:*advanced:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:*express:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:*standard:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:*advanced:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:*express:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:*standard:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:cf2:*:*:*advanced:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:cf2:*:*:*express:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:cf2:*:*:*standard:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*:*advanced:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*:*express:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*:*standard:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.2:*:*:*advanced:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.2:*:*:*express:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.6.2:*:*:*standard:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:*:*:*advanced:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:*:*:*express:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:*:*:*standard:*:*:						
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201606:*:*:*advanced:*:*:						

cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201606:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201606:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201609:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201609:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201609:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201612:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201612:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201612:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201703:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201703:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201703:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201706:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201706:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201706:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.6.0.0:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.6.0.0:cf201712:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:cf2:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:cf2:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:cf2:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*:advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*:standard:*:*:

cpe:2.3:a:ibm:business_process_manager:8.5.6.2:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.2:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.2:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201606:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201606:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201606:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201609:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201609:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201609:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201612:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201612:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201612:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201703:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201703:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201703:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201706:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201706:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.7.0:cf201706:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.6.0.0:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.6.0.0:cf201712:*:*express:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)