

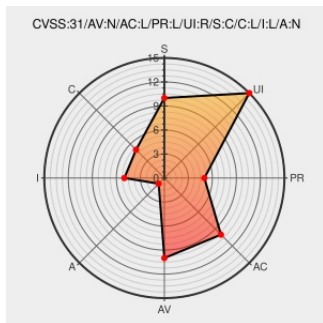


CVE-2020-4516

Published on: 09/08/2020 12:00:00 AM UTC

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

CVE-2020-4516

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

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

IBM Business Process Manager 8.5, 8.6 and IBM Business Automation Workflow 18.0, 19.0, and 20.0 are 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:

182371.

CVE-2020-4516 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 **8.5**

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

Affected Vendor/Software: [IBM](#) - **Business Automation Workflow** version **18.0**

Affected Vendor/Software: [IBM](#) - **Business Automation Workflow** version **19.0**

Affected Vendor/Software: [IBM](#) - **Business Automation Workflow** version **20.0**

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: Cross-site scripting vulnerability affects IBM Business Automation Workflow and IBM Business Process Manager (BPM) - CVE-2020-4516	Patch Vendor Advisory www.ibm.com text/html	 CONFIRM www.ibm.com/support/pages/node/6326901
IBM X-Force Exchange	VDB Entry Vendor Advisory exchange.xforce.ibmcloud.com text/html	 XF ibm-bpm-cve20204516-xss (182371)

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 Automation Workflow	18.0.0.0	All	All	All
Application	Ibm	Business Automation Workflow	18.0.0.1	All	All	All
Application	Ibm	Business Automation Workflow	18.0.0.2	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.0	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.1	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.2	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.3	All	All	All
Application	Ibm	Business Automation Workflow	20.0.0.1	All	All	All
Application	Ibm	Business Automation Workflow	18.0.0.0	All	All	All
Application	Ibm	Business Automation Workflow	18.0.0.1	All	All	All
Application	Ibm	Business Automation Workflow	18.0.0.2	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.0	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.1	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.2	All	All	All
Application	Ibm	Business Automation Workflow	19.0.0.3	All	All	All
Application	Ibm	Business Automation Workflow	20.0.0.1	All	All	All
Application	Ibm	Business Process Manager	8.5.0.0	All	All	All

[illegible]

Application	lbn	Business Process Manager	8.5.6.0	-	All	All
Application	lbn	Business Process Manager	8.5.6.1	All	All	All
Application	lbn	Business Process Manager	8.5.6.1	All	All	All
Application	lbn	Business Process Manager	8.5.6.2	All	All	All
Application	lbn	Business Process Manager	8.5.6.2	All	All	All
Application	lbn	Business Process Manager	8.5.7.0	All	All	All
Application	lbn	Business Process Manager	8.5.7.0	All	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201606	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201606	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201609	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201609	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201612	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201612	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201703	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201703	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201706	All	All
Application	lbn	Business Process Manager	8.5.7.0	cf201706	All	All
Application	lbn	Business Process Manager	8.6.0.0	-	All	All
Application	lbn	Business Process Manager	8.6.0.0	-	All	All
cpe:2.3:a:ibm:business_automation_workflow:18.0.0.0:*****:						
cpe:2.3:a:ibm:business_automation_workflow:18.0.0.1:*****:						
cpe:2.3:a:ibm:business_automation_workflow:18.0.0.2:*****:						
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.0:*****:						
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.1:*****:						
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.2:*****:						
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.3:*****:						
cpe:2.3:a:ibm:business_automation_workflow:20.0.0.1:*****:						
cpe:2.3:a:ibm:business_automation_workflow:18.0.0.0:*****:						
cpe:2.3:a:ibm:business_automation_workflow:18.0.0.1:*****:						
cpe:2.3:a:ibm:business_automation_workflow:18.0.0.2:*****:						
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.0:*****:						
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.1:*****:						

cpe:2.3:a:ibm:business_automation_workflow:19.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:business_automation_workflow:19.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:business_automation_workflow:20.0.0.1:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.2:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.2:*:*:standard:*:*:
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:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.2:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.0.2:*:*:standard:*:*:
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:*:*:express:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.0:*:*:standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.5.6.1:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:*:*: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:-:*:*:standard:*:*:

No vendor comments have been submitted for this CVE

[← 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](#)