

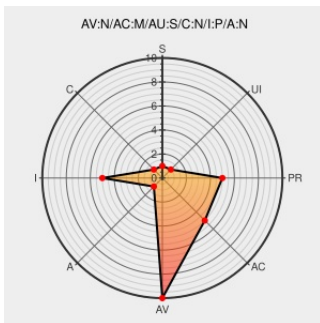


CVE-2015-1906

Published on: 07/21/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1906

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

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

Cross-site scripting (XSS) vulnerability in the REST API in IBM Business Process Manager (BPM) 7.5.x through 7.5.1.2, 8.0.x through 8.0.1.3, 8.5.0 through 8.5.0.1, 8.5.5 through 8.5.5.0, and 8.5.6 through 8.5.6.0 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.

CVE-2015-1906 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **3.5 - LOW**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

SINGLE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

IBM Security Bulletin: Insufficient authorization in Service REST API and cross site scripting vulnerability in REST API affecting IBM Business Process Manager (CVE-2015-1905, CVE-2015-1906) - United States

[Patch](#)
[Vendor Advisory](#)
[www-01.ibm.com](#)
[text/html](#)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21700717](#)

IBM JR52772: SECURITY APAR - CVE-2015-1905, CVE-2015-1906 - MULTIPLE VULNERABILITIES IN IBM BUSINESS PROCESS MANAGER REST API - United States

[Patch](#)
[Vendor Advisory](#)
[www-01.ibm.com](#)
[text/html](#)

[AIXAPAR JR52772](#)

IBM Business Process Manager Bugs Let Remote Users Conduct Cross-Site Scripting Attacks and Remote Authenticated Users Modify Data on the Target System - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTRAK 1033002](#)

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	7.5.0.0	All	All	All
Application	ibm	Business Process Manager	7.5.0.0	All	All	All
Application	ibm	Business Process Manager	7.5.0.0	All	All	All
Application	ibm	Business Process Manager	7.5.0.0	All	All	All
Application	ibm	Business Process Manager	7.5.0.1	All	All	All
Application	ibm	Business Process Manager	7.5.0.1	All	All	All
Application	ibm	Business Process Manager	7.5.0.1	All	All	All
Application	ibm	Business Process Manager	7.5.0.1	All	All	All
Application	ibm	Business Process Manager	7.5.1.0	All	All	All
Application	ibm	Business Process Manager	7.5.1.0	All	All	All
Application	ibm	Business Process Manager	7.5.1.0	All	All	All
Application	ibm	Business Process Manager	7.5.1.0	All	All	All
Application	ibm	Business Process Manager	7.5.1.1	All	All	All
Application	ibm	Business Process Manager	7.5.1.1	All	All	All
Application	ibm	Business Process Manager	7.5.1.1	All	All	All
Application	ibm	Business Process Manager	7.5.1.1	All	All	All
Application	ibm	Business Process Manager	7.5.1.1	All	All	All
Application	ibm	Business Process Manager	7.5.1.2	All	All	All
Application	ibm	Business Process Manager	7.5.1.2	All	All	All
Application	ibm	Business Process Manager	7.5.1.2	All	All	All
Application	ibm	Business Process Manager	7.5.1.2	All	All	All
Application	ibm	Business Process Manager	8.0.0.0	All	All	All
Application	ibm	Business Process Manager	8.0.0.0	All	All	All
Application	ibm	Business Process Manager	8.0.0.0	All	All	All
Application	ibm	Business Process Manager	8.0.0.0	All	All	All
Application	ibm	Business Process Manager	8.0.1.0	All	All	All
Application	ibm	Business Process Manager	8.0.1.0	All	All	All
Application	ibm	Business Process Manager	8.0.1.0	All	All	All
Application	ibm	Business Process Manager	8.0.1.0	All	All	All

[illegible]

[illegible]

Application	ibm	Business Process Manager	8.5.0.1	All	All	All
Application	ibm	Business Process Manager	8.5.0.1	All	All	All
Application	ibm	Business Process Manager	8.5.0.1	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	8.5.5.0	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	All	All	All
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:***:***:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:***:advanced:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:***:express:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:***:standard:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:***:***:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:***:advanced:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:***:express:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:***:standard:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:***:***:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:***:advanced:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:***:express:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:***:standard:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:***:***:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:***:advanced:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:***:express:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:***:standard:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:***:***:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:***:advanced:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:***:express:***:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:***:standard:***:						

cpe:2.3:a:ibm:business_process_manager:8.0.0.0:****:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:****:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:****:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:****:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.3:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.3:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.3:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:****:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:***:advanced:***:
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:****:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:***:advanced:***:
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:8.5.5.0:****:

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:*:*:*:*:*:
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:7.5.0.0:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:*:*:*advanced:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:*:*:*express:*:*:
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:*:*:*standard:*:*:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:*:*:*:*:*:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:*:*:*advanced:*:*:

cpe:2.3:a:ibm:business_process_manager:8.0.0.0:1:1:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:***:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:***:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:***:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.3:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.3:***:express:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.3:***:standard:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:***:***:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:***:advanced:***:
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:***:***:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:***:advanced:***:
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:8.5.5.0:***:***:***:
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:*:*:*:*:*:
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:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →