



CVE-2014-3075

Published on: 09/04/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

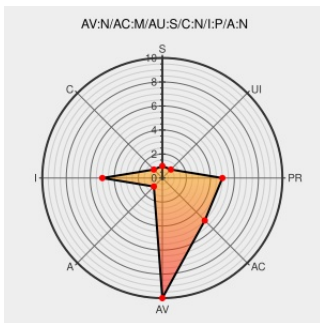
CVE-2014-3075

[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 IBM Business Process Manager (BPM) 7.5.x through 8.5.5 and WebSphere Lombardi Edition 7.2.0.x allows remote authenticated users to inject arbitrary web script or HTML via an uploaded file.

CVE-2014-3075 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

JR50092: THE FILE MIME TYPE IS NOT VALIDATED FOR DOCUMENTS CREATED OR UPDATED FROM THE DOCUMENT LIST COACH VIEW

Security Bulletin: Insufficient control over MIME types in Business Process Manager (BPM) and WebSphere Lombardi Edition document feature (CVE-2014-3075)

IBM X-Force Exchange

Tags

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

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

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

Link

[AIXAPAR JR50092](#)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21679979](#)

[XF ibm-websphere-cve20143075-file-upload\(93817\)](#)

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

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	7.5.0.1	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	7.5.1.2	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	8.0.1.1	All	All	All
Application	IBM	Business Process Manager	8.0.1.2	All	All	All
Application	IBM	Business Process Manager	8.5.0.0	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	7.5.0.0	All	All	All
Application	IBM	Business Process Manager	7.5.0.1	All	All	All
Application	IBM	Business Process Manager	7.5.1.0	All	All	All
Application	IBM	Business Process Manager	7.5.1.1	All	All	All
Application	IBM	Business Process Manager	7.5.1.2	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	8.0.1.1	All	All	All
Application	IBM	Business Process Manager	8.0.1.2	All	All	All
Application	IBM	Business Process Manager	8.5.0.0	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	Websphere Application Server	7.2	All	All	All
Application	IBM	Websphere Application Server	7.2.0.1	All	All	All
Application	IBM	Websphere Application Server	7.2.0.2	All	All	All
Application	IBM	Websphere Application Server	7.2.0.3	All	All	All
Application	IBM	Websphere Application Server	7.2.0.4	All	All	All
Application	IBM	Websphere Application Server	7.2.0.5	All	All	All

Application	ibm	Websphere Application Server	7.2	All	All	All
Application	ibm	Websphere Application Server	7.2.0.1	All	All	All
Application	ibm	Websphere Application Server	7.2.0.2	All	All	All
Application	ibm	Websphere Application Server	7.2.0.3	All	All	All
Application	ibm	Websphere Application Server	7.2.0.4	All	All	All
Application	ibm	Websphere Application Server	7.2.0.5	All	All	All
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:*****:						
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:*****:						
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:*****:						
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:*****:						
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:*****:						
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:*****:						
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:*****:						
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:*****:						

cpe:2.3:a:ibm:business_process_manager:8.5.5.0:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.1:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.2:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.3:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.4:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.5:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.1:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.2:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.3:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.4:*:*:*:lombardi:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.2.0.5:*:*:*:lombardi:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)