



CVE-2014-6101

Published on: 10/31/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:54 PM UTC

CVE-2014-6101

[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 redirect-login feature in IBM Business Process Manager (BPM) Advanced 7.5 through 8.5.5 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.

CVE-2014-6101 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

JR51507: SECURITY APAR CVE-2014-6101 - CROSS-SITE-SCRIPTING VULNERABILITY IN IBM BPM WHEN YOU USE REDIRECT-LOGIN MECHANISM

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

[AIXAPAR JR51507](#)

Security Bulletin: Cross-site scripting vulnerability in IBM Business Process Manager (BPM) redirect-login mechanism (CVE-2014-6101)

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

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21687967](#)

JR51211: SECURITY APAR CVE-2014-6101 - CROSS-SITE-SCRIPTING VULNERABILITY IN IBM BPM WHEN YOU USE REDIRECT-LOGIN MECHANISM

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

[AIXAPAR JR51211](#)

About Secunia Research | Flexera

[secunia.com](#)
[Deprecated Link](#)
[text/html](#)

[SECUNIA 61804](#)

There are currently no QIDs associated with this CVE

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

```
cpe:2.3:a:ibm:business process manager:7.5.0.1::*:advanced::*
```

cpe:2.3:a:ibm:business_process_manager:7.5.1.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.0.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.0.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.1.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.1.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:7.5.1.2:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.0.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.0.1.2:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.0:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.5.0.1:***:advanced:***:
cpe:2.3:a:ibm:business_process_manager:8.5.5.0:***:advanced:***:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)