



CVE-2015-2013

Published on: 09/13/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:20 PM UTC

CVE-2015-2013

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

Certain versions of [Websphere Mq](#) from [Ibm](#) contain the following vulnerability:

IBM WebSphere MQ 7.0.1 before 7.0.1.13 allows remote attackers to cause a denial of service (channel-agent abend and process outage) via a crafted selection string in an MQI call.

CVE-2015-2013 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM Security Bulletin: IBM WebSphere MQ 7.0.1 potential denial of service (CVE-2015-2013) - United States

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[CONFIRM](#) www-01.ibm.com/support/docview.wss?uid=swg21962479

IBM notice: The page you requested cannot be displayed

[www-01.ibm.com](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[AIXAPAR IV73860](#)

IBM WebSphere MQ MQI Call Processing Flaw Lets Remote Users Cause the Target Channel Agent to Crash - SecurityTracker

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

[SECTrack 1033449](#)

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	Websphere Mq	7.0.1.0	All	All	All
Application	Ibm	Websphere Mq	7.0.1.1	All	All	All
Application	Ibm	Websphere Mq	7.0.1.10	All	All	All
Application	Ibm	Websphere Mq	7.0.1.11	All	All	All
Application	Ibm	Websphere Mq	7.0.1.12	All	All	All
Application	Ibm	Websphere Mq	7.0.1.2	All	All	All
Application	Ibm	Websphere Mq	7.0.1.3	All	All	All
Application	Ibm	Websphere Mq	7.0.1.4	All	All	All
Application	Ibm	Websphere Mq	7.0.1.5	All	All	All
Application	Ibm	Websphere Mq	7.0.1.6	All	All	All
Application	Ibm	Websphere Mq	7.0.1.7	All	All	All
Application	Ibm	Websphere Mq	7.0.1.8	All	All	All
Application	Ibm	Websphere Mq	7.0.1.9	All	All	All
Application	Ibm	Websphere Mq	7.0.1.0	All	All	All
Application	Ibm	Websphere Mq	7.0.1.1	All	All	All
Application	Ibm	Websphere Mq	7.0.1.10	All	All	All
Application	Ibm	Websphere Mq	7.0.1.11	All	All	All
Application	Ibm	Websphere Mq	7.0.1.12	All	All	All
Application	Ibm	Websphere Mq	7.0.1.2	All	All	All
Application	Ibm	Websphere Mq	7.0.1.3	All	All	All
Application	Ibm	Websphere Mq	7.0.1.4	All	All	All
Application	Ibm	Websphere Mq	7.0.1.5	All	All	All
Application	Ibm	Websphere Mq	7.0.1.6	All	All	All
Application	Ibm	Websphere Mq	7.0.1.7	All	All	All
Application	Ibm	Websphere Mq	7.0.1.8	All	All	All
Application	Ibm	Websphere Mq	7.0.1.9	All	All	All

```
cpe:2.3:a:ibm:websphere_mq:7.0.1.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_mq:7.0.1.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere mq:7.0.1.10:::~::~:
```

cpe:2.3:a:ibm:websphere_mq:7.0.1.11:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.12:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.2:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.3:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.4:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.5:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.6:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.7:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.8:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.9:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.0:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.1:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.10:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.11:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.12:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.2:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.3:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.4:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.5:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.6:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.7:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.8:*****:
cpe:2.3:a:ibm:websphere_mq:7.0.1.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

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](#)