



CVE-2013-5372

Published on: 10/19/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:35 PM UTC

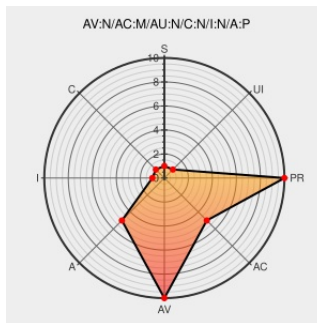
CVE-2013-5372

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The XML4J parser in IBM WebSphere Message Broker 6.1 before 6.1.0.12, 7.0 before 7.0.0.7, and 8.0 before 8.0.0.4 and IBM Integration Bus 9.0 before 9.0.0.1 allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document that triggers expansion for many entities.

CVE-2013-5372 has been assigned by psirt@us.ibm.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

IBM Security
Bulletin: Multiple
vulnerabilities in
IBM WebSphere
Real Time - United
States

[www-01.ibm.com
text/html](http://www-01.ibm.com/text/html)

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21655202](http://www-01.ibm.com/support/docview.wss?uid=swg21655202)

IBM WebSphere
Message Broker
and IBM Integration
Bus Security
Vulnerability:
XML4J denial of
service attack
(CVE-2013-5372) -

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

[CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21653087](http://www-01.ibm.com/support/docview.wss?uid=swg21653087)

United States		
developerWorks : Technical Topics : Java™ technology : IBM Developer kits : Security alerts	www.ibm.com text/html Inactive Link Not Archived	 CONFIRM www.ibm.com/developerworks/java/jdk/alerts/#IBM_Security_Update_November_2013
IBM notice: The page you requested cannot be displayed	www-01.ibm.com text/html Inactive Link Not Archived	 AIXAPAR IC96473
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1508
Security Advisory SA56338 - IBM Smart Analytics System Series Java Multiple Vulnerabilities - Secunia	web.archive.org text/html	 SECUNIA 56338
IBM Security Bulletin: Multiple vulnerabilities in current releases of the IBM® SDK, Java™ Technology Edition - United States	www-01.ibm.com text/html	 CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21655201
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1793
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF ibm-xml4j-cve20135372-dos(86662)
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1507
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:1509
[security-announce] SUSE-SU- 2013:1677-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2013:1677
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	Websphere Message Broker	6.1	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.1	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.10	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.11	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.2	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.3	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.4	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.5	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.6	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.7	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.8	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.9	All	All	All
Application	Ibm	Websphere Message Broker	7.0.	All	All	All
Application	Ibm	Websphere Message Broker	7.0.0.1	All	All	All
Application	Ibm	Websphere Message Broker	7.0.0.2	All	All	All
Application	Ibm	Websphere Message Broker	7.0.0.3	All	All	All
Application	Ibm	Websphere Message Broker	7.0.0.4	All	All	All
Application	Ibm	Websphere Message Broker	7.0.0.5	All	All	All
Application	Ibm	Websphere Message Broker	7.0.0.6	All	All	All
Application	Ibm	Websphere Message Broker	8.0	All	All	All
Application	Ibm	Websphere Message Broker	8.0.0.1	All	All	All
Application	Ibm	Websphere Message Broker	8.0.0.2	All	All	All
Application	Ibm	Websphere Message Broker	8.0.0.3	All	All	All
Application	Ibm	Websphere Message Broker	6.1	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.1	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.10	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.11	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.2	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.3	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.4	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.5	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.6	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.7	All	All	All
Application	Ibm	Websphere Message Broker	6.1.0.8	All	All	All

Application	ibm	Websphere Message Broker	6.1.0.9	All	All	All
Application	ibm	Websphere Message Broker	7.0.	All	All	All
Application	ibm	Websphere Message Broker	7.0.0.1	All	All	All
Application	ibm	Websphere Message Broker	7.0.0.2	All	All	All
Application	ibm	Websphere Message Broker	7.0.0.3	All	All	All
Application	ibm	Websphere Message Broker	7.0.0.4	All	All	All
Application	ibm	Websphere Message Broker	7.0.0.5	All	All	All
Application	ibm	Websphere Message Broker	7.0.0.6	All	All	All
Application	ibm	Websphere Message Broker	8.0	All	All	All
Application	ibm	Websphere Message Broker	8.0.0.1	All	All	All
Application	ibm	Websphere Message Broker	8.0.0.2	All	All	All
Application	ibm	Websphere Message Broker	8.0.0.3	All	All	All
cpe:2.3:a:ibm:websphere_message_broker:6.1.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.1.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.10.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.11.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.2.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.3.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.4.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.5.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.6.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.7.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.8.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.9.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.1.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.2.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.3.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.4.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.5.*.*.*.*.*.*:						
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.6.*.*.*.*.*.*:						

```
cpe:2.3:a:ibm:websphere_message_broker:8.0:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_message_broker:8.0.0.1:*.:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:8.0.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_message_broker:8.0.0.3:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_message_broker:6.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.1:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.10:*:*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere message broker:6.1.0.11:*.~*~*~*~*~*~*
```

cpe:2.3:a:ibm:websphere_message_broker:6.1.0.2:*:*:*:*:*

```
cpe:2.3:a:ibm:websphere message broker:6.1.0.3.*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.4:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.5:::*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.6:::*:*:*.*
```

cpe:2.3:a:ibm:websphere_message_broker:6.1.0.7:::*:*:*:*.*

cpe:2.3:a:ibm:websphere_message_broker:6.1.0.8:*:*:*:*:*

```
cpe:2.3:a:ibm:websphere_message_broker:6.1.0.9:::*:*:*.*
```

```
cpe:2.3:a:ibm:websphere:message_broker:7.0.:*:~::~
```

```
cpe:2.3:a:ibm:websphere message broker:7.0.0.1:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.2:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere message broker:7.0.0.3:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:ibm:websphere message broker:7.0.0.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.5:::*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:7.0.0.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_message_broker:8.0:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere message broker:8.0.0.1:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:8.0.0.2:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_message_broker:8.0.0.3:::*:*:*:*.*
```

No vendor comments have been submitted for this CVE

© [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](#)