

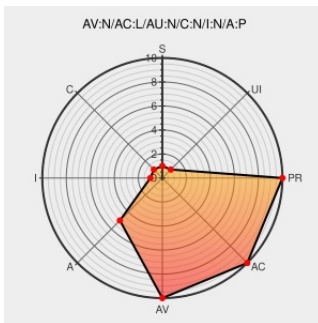


CVE-2011-1317

Published on: 03/08/2011 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:16 PM UTC

CVE-2011-1317

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

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

Memory leak in `com.ibm.ws.jsp.runtime.WASJSPStrBufferImpl` in the JavaServer Pages (JSP) component in IBM WebSphere Application Server (WAS) 6.1.0.x before 6.1.0.37 and 7.x before 7.0.0.15 allows remote attackers to cause a denial of service (memory consumption) by sending many JSP requests that trigger large responses.

CVE-2011-1317 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
IBM Fix list for IBM WebSphere Application Server V7.0 - United States	Patch Vendor Advisory www-01.ibm.com text/html	CONFIRM www-01.ibm.com/support/docview.wss?uid=swg27014463
PM19500: OUTFOMEMORY OCCUR DUE TO LEAK OF COM.IBM.WS.JSP.RUNTIME.WASJSPSTRBUFFERIMPL	Vendor Advisory www-01.ibm.com text/html	AIXAPAR PM19500

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 Application Server	6.1.0	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.0	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.1	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.11	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.12	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.15	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.17	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.19	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.2	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.21	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.23	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.25	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.27	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.29	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.3	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.31	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.33	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.35	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.5	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.7	All	All	All
Application	IBM	WebSphere Application Server	6.1.0.9	All	All	All
Application	IBM	WebSphere Application Server	7.0	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.1	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.11	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.13	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.2	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.3	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.4	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.5	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.6	All	All	All
Application	IBM	WebSphere Application Server	7.0.0.7	All	All	All

[illegible]

cpe:2.3:a:ibm:websphere_application_server:6.1.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.12:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.15:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.29:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.31:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.33:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.35:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.5:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*****:
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.1:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.11:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*****:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*****:

```
cpe:2.3:a:ibm:websphere application server:7.0.0.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere application server:7.0.0.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0:*.:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.0:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.11:::*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere application server:6.1.0.12:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere application server:6.1.0.15:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.17:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.19:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.2:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.21:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.23:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.25:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.27:*:*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.29:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.3:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.31:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.33:::*:*:*.*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.35:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere application server:6.1.0.5:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.7:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:6.1.0.9:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0:*:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.1:::*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_application_server:7.0.0.11:::*:*:*.*.*
```

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

cpe:2.3:a:ibm:websphere_application_server:7.0.0.13:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.2:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.3:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.4:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.5:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.6:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.7:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.8:*:*:*:*:*:
cpe:2.3:a:ibm:websphere_application_server:7.0.0.9:*:*:*:*:*:

[← Previous ID](#)

Next ID→

© 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