

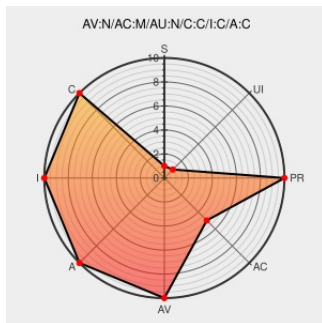


# CVE-2013-3009

Published on: 07/23/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

## CVE-2013-3009

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

Certain versions of [Java](#) from [ibm](#) contain the following vulnerability:

The `com.ibm.CORBA.iiop.ClientDelegate` class in IBM Java 1.4.2 before 1.4.2 SR13-FP18, 5.0 before 5.0 SR16-FP3, 6 before 6 SR14, 6.0.1 before 6.0.1 SR6, and 7 before 7 SR5 improperly exposes the `invoke` method of the `java.lang.reflect.Method` class, which allows remote attackers to call `setSecurityManager` and bypass a sandbox protection mechanism via vectors related to the `AccessController`

`doPrivileged` block.

CVE-2013-3009 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>COMPLETE</b>        | <b>COMPLETE</b>   | <b>COMPLETE</b>     |

## CVE References

| Description                                                             | Tags                                                                                                                            | Link                                   |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|
| About Secunia Research   Flexera                                        | <a href="#">Vendor Advisory</a><br><a href="#">secunia.com</a><br><a href="#">Deprecated Link</a><br><a href="#">text/plain</a> | <a href="#">X SECUNIA 54154</a>        |
| [security-announce] SUSE-SU-2013:1263-1: important: Security update for | <a href="#">lists.opensuse.org</a><br><a href="#">text/html</a>                                                                 | <a href="#">SUSE SUSE-SU-2013:1263</a> |
| IBM PM91727: FIX SECURITY VULNERABILITY CVE-2013-3009 - United          | <a href="#">www-01.ibm.com</a><br><a href="#">text/html</a>                                                                     | <a href="#">AIXAPAR PM91727</a>        |

|                                                                                                                            |                                                                                                                                                                                   |                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2013-3009 - United States                                                                                                  |                                                                                                                                                                                   |                                                                                                                                                                        |
| [security-announce]<br>SUSE-SU-2013:1255-1:<br>important: Security<br>update for                                           | <a href="https://lists.opensuse.org/text/html">lists.opensuse.org</a><br><a href="https://lists.opensuse.org/text/html">text/html</a>                                             |  <a href="#">SUSE SUSE-SU-2013:1255</a>                                               |
| IBM Security Bulletin:<br>Rational Host On-<br>Demand clients affected<br>by vulnerabilities in IBM<br>JRE - United States | <a href="#">Vendor Advisory</a><br><a href="http://www-01.ibm.com">www-01.ibm.com</a><br><a href="#">text/html</a>                                                                |  <a href="#">CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21644197</a>           |
| IBM IX90118: FIX<br>SECURITY<br>VULNERABILITY CVE-<br>2013-3009 - United<br>States                                         | <a href="http://www-01.ibm.com">www-01.ibm.com</a><br><a href="#">text/html</a>                                                                                                   |  <a href="#">AIXAPAR IX90118</a>                                                      |
| IBM X-Force Exchange                                                                                                       | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a><br><a href="#">text/html</a>                                                                      |  <a href="#">XF ibm-java-cve20133009(84150)</a>                                       |
| Security Explorations                                                                                                      | <a href="http://www.security-explorations.com">www.security-explorations.com</a><br><a href="#">application/pdf</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  <a href="#">MISC www.security-explorations.com/materials/SE-2012-01-IBM-2.pdf</a>    |
| [security-announce]<br>SUSE-SU-2013:1257-1:<br>important: Security<br>update for                                           | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br><a href="https://lists.opensuse.org/text/html">text/html</a>                                                       |  <a href="#">SUSE SUSE-SU-2013:1257</a>                                               |
| [security-announce]<br>SUSE-SU-2013:1264-1:<br>important: Security<br>update for                                           | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br><a href="https://lists.opensuse.org/text/html">text/html</a>                                                       |  <a href="#">SUSE SUSE-SU-2013:1264</a>                                             |
| [security-announce]<br>SUSE-SU-2013:1293-1:<br>important: Security<br>update for                                           | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br><a href="https://lists.opensuse.org/text/html">text/html</a>                                                       |  <a href="#">SUSE SUSE-SU-2013:1293</a>                                             |
| Security Explorations                                                                                                      | <a href="http://www.security-explorations.com">www.security-explorations.com</a><br><a href="#">application/pdf</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  <a href="#">MISC www.security-explorations.com/materials/SE-2012-01-IBM-4.pdf</a>  |
| IBM IV44792: FIX<br>SECURITY<br>VULNERABILITY CVE-<br>2013-3009 - United<br>States                                         | <a href="http://www-01.ibm.com">www-01.ibm.com</a><br><a href="#">text/html</a>                                                                                                   |  <a href="#">AIXAPAR IV44792</a>                                                    |
| IBM Security Bulletin:<br>Multiple vulnerabilities in<br>IBM WebSphere Real<br>Time - United States                        | <a href="#">Vendor Advisory</a><br><a href="http://www-01.ibm.com">www-01.ibm.com</a><br><a href="#">text/html</a>                                                                |  <a href="#">CONFIRM www-01.ibm.com/support/docview.wss?uid=swg21642336</a>         |
| [security-announce]<br>SUSE-SU-2013:1256-1:<br>important: Security<br>update for                                           | <a href="https://lists.opensuse.org">lists.opensuse.org</a><br><a href="https://lists.opensuse.org/text/html">text/html</a>                                                       |  <a href="#">SUSE SUSE-SU-2013:1256</a>                                             |
| Full Disclosure: [SE-<br>2012-01] Broken security<br>fix in IBM Java 7/8                                                   | <a href="https://seclists.org">seclists.org</a><br><a href="#">text/html</a>                                                                                                      |  <a href="#">FULLDISC 20160404 [SE-2012-01] Broken security fix in IBM Java 7/8</a> |
| Red Hat Customer Portal                                                                                                    | <a href="https://web.archive.org">web.archive.org</a><br><a href="#">text/html</a>                                                                                                |  <a href="#">REDHAT RHSA-2013:1060</a>                                              |

Inactive Link Not Archived

[security-announce]  
SUSE-SU-2013:1305-1:  
important: Security  
update for

lists.opensuse.org  
text/html

 SUSE SUSE-SU-2013:1305

Red Hat Customer Portal

web.archive.org  
text/html

 REDHAT RHSA-2013:1081

Inactive Link Not Archived

Full Disclosure: Re: [SE-  
2012-01] Broken security  
fix in IBM Java 7/8

seclists.org  
text/html

 FULLDISC 20160405 Re: [SE-2012-01] Broken security fix in IBM Java 7/8

developerWorks :  
Technical Topics : Java™  
technology : IBM  
Developer kits : Security  
alerts

Vendor Advisory  
www.ibm.com  
text/html

 CONFIRM  
www.ibm.com/developerworks/java/jdk/alerts/#IBM\_Security\_Update\_July\_2013

Red Hat Customer Portal

web.archive.org  
text/html

 REDHAT RHSA-2013:1059

Inactive Link Not Archived

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](mailto: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    | Java    | 1.4.2       | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13    | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.1  | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.10 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.11 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.12 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.13 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.14 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.15 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.16 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.17 | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.2  | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.3  | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.4  | All    | All     | All      |
| Application | ibm    | Java    | 1.4.2.13.5  | All    | All     | All      |

|             |     |      |            |     |     |     |
|-------------|-----|------|------------|-----|-----|-----|
| Application | lbm | Java | 1.4.2.13.6 | All | All | All |
| Application | lbm | Java | 1.4.2.13.7 | All | All | All |
| Application | lbm | Java | 1.4.2.13.8 | All | All | All |
| Application | lbm | Java | 1.4.2.13.9 | All | All | All |
| Application | lbm | Java | 5.0.0.0    | All | All | All |
| Application | lbm | Java | 5.0.11.0   | All | All | All |
| Application | lbm | Java | 5.0.11.1   | All | All | All |
| Application | lbm | Java | 5.0.11.2   | All | All | All |
| Application | lbm | Java | 5.0.12.0   | All | All | All |
| Application | lbm | Java | 5.0.12.1   | All | All | All |
| Application | lbm | Java | 5.0.12.2   | All | All | All |
| Application | lbm | Java | 5.0.12.3   | All | All | All |
| Application | lbm | Java | 5.0.12.4   | All | All | All |
| Application | lbm | Java | 5.0.12.5   | All | All | All |
| Application | lbm | Java | 5.0.13.0   | All | All | All |
| Application | lbm | Java | 5.0.14.0   | All | All | All |
| Application | lbm | Java | 5.0.15.0   | All | All | All |
| Application | lbm | Java | 5.0.16.0   | All | All | All |
| Application | lbm | Java | 5.0.16.1   | All | All | All |
| Application | lbm | Java | 5.0.16.2   | All | All | All |
| Application | lbm | Java | 6.0.0.0    | All | All | All |
| Application | lbm | Java | 6.0.1.0    | All | All | All |
| Application | lbm | Java | 6.0.10.0   | All | All | All |
| Application | lbm | Java | 6.0.10.1   | All | All | All |
| Application | lbm | Java | 6.0.11.0   | All | All | All |
| Application | lbm | Java | 6.0.12.0   | All | All | All |
| Application | lbm | Java | 6.0.13.0   | All | All | All |
| Application | lbm | Java | 6.0.13.1   | All | All | All |
| Application | lbm | Java | 6.0.13.2   | All | All | All |
| Application | lbm | Java | 6.0.2.0    | All | All | All |
| Application | lbm | Java | 6.0.3.0    | All | All | All |
| Application | lbm | Java | 6.0.4.0    | All | All | All |
| Application | lbm | Java | 6.0.5.0    | All | All | All |
| Application | lbm | Java | 6.0.6.0    | All | All | All |
| Application | lbm | Java | 6.0.7.0    | All | All | All |

|             |     |      |             |     |     |     |
|-------------|-----|------|-------------|-----|-----|-----|
| Application | lbm | Java | 6.0.8.0     | All | All | All |
| Application | lbm | Java | 6.0.8.1     | All | All | All |
| Application | lbm | Java | 6.0.9.0     | All | All | All |
| Application | lbm | Java | 6.0.9.1     | All | All | All |
| Application | lbm | Java | 6.0.9.2     | All | All | All |
| Application | lbm | Java | 7.0.0.0     | All | All | All |
| Application | lbm | Java | 7.0.1.0     | All | All | All |
| Application | lbm | Java | 7.0.2.0     | All | All | All |
| Application | lbm | Java | 7.0.3.0     | All | All | All |
| Application | lbm | Java | 7.0.4.0     | All | All | All |
| Application | lbm | Java | 7.0.4.1     | All | All | All |
| Application | lbm | Java | 7.0.4.2     | All | All | All |
| Application | lbm | Java | 1.4.2       | All | All | All |
| Application | lbm | Java | 1.4.2.13    | All | All | All |
| Application | lbm | Java | 1.4.2.13.1  | All | All | All |
| Application | lbm | Java | 1.4.2.13.10 | All | All | All |
| Application | lbm | Java | 1.4.2.13.11 | All | All | All |
| Application | lbm | Java | 1.4.2.13.12 | All | All | All |
| Application | lbm | Java | 1.4.2.13.13 | All | All | All |
| Application | lbm | Java | 1.4.2.13.14 | All | All | All |
| Application | lbm | Java | 1.4.2.13.15 | All | All | All |
| Application | lbm | Java | 1.4.2.13.16 | All | All | All |
| Application | lbm | Java | 1.4.2.13.17 | All | All | All |
| Application | lbm | Java | 1.4.2.13.2  | All | All | All |
| Application | lbm | Java | 1.4.2.13.3  | All | All | All |
| Application | lbm | Java | 1.4.2.13.4  | All | All | All |
| Application | lbm | Java | 1.4.2.13.5  | All | All | All |
| Application | lbm | Java | 1.4.2.13.6  | All | All | All |
| Application | lbm | Java | 1.4.2.13.7  | All | All | All |
| Application | lbm | Java | 1.4.2.13.8  | All | All | All |
| Application | lbm | Java | 1.4.2.13.9  | All | All | All |
| Application | lbm | Java | 5.0.0.0     | All | All | All |
| Application | lbm | Java | 5.0.11.0    | All | All | All |
| Application | lbm | Java | 5.0.11.1    | All | All | All |
| Application | lbm | Java | 5.0.11.2    | All | All | All |
| Application | lbm | Java | 5.0.12.0    | All | All | All |

|             |     |      |          |     |     |     |
|-------------|-----|------|----------|-----|-----|-----|
| Application | IBM | Java | 5.0.12.0 | All | All | All |
| Application | IBM | Java | 5.0.12.1 | All | All | All |
| Application | IBM | Java | 5.0.12.2 | All | All | All |
| Application | IBM | Java | 5.0.12.3 | All | All | All |
| Application | IBM | Java | 5.0.12.4 | All | All | All |
| Application | IBM | Java | 5.0.12.5 | All | All | All |
| Application | IBM | Java | 5.0.13.0 | All | All | All |
| Application | IBM | Java | 5.0.14.0 | All | All | All |
| Application | IBM | Java | 5.0.15.0 | All | All | All |
| Application | IBM | Java | 5.0.16.0 | All | All | All |
| Application | IBM | Java | 5.0.16.1 | All | All | All |
| Application | IBM | Java | 5.0.16.2 | All | All | All |
| Application | IBM | Java | 6.0.0.0  | All | All | All |
| Application | IBM | Java | 6.0.1.0  | All | All | All |
| Application | IBM | Java | 6.0.10.0 | All | All | All |
| Application | IBM | Java | 6.0.10.1 | All | All | All |
| Application | IBM | Java | 6.0.11.0 | All | All | All |
| Application | IBM | Java | 6.0.12.0 | All | All | All |
| Application | IBM | Java | 6.0.13.0 | All | All | All |
| Application | IBM | Java | 6.0.13.1 | All | All | All |
| Application | IBM | Java | 6.0.13.2 | All | All | All |
| Application | IBM | Java | 6.0.2.0  | All | All | All |
| Application | IBM | Java | 6.0.3.0  | All | All | All |
| Application | IBM | Java | 6.0.4.0  | All | All | All |
| Application | IBM | Java | 6.0.5.0  | All | All | All |
| Application | IBM | Java | 6.0.6.0  | All | All | All |
| Application | IBM | Java | 6.0.7.0  | All | All | All |
| Application | IBM | Java | 6.0.8.0  | All | All | All |
| Application | IBM | Java | 6.0.8.1  | All | All | All |
| Application | IBM | Java | 6.0.9.0  | All | All | All |
| Application | IBM | Java | 6.0.9.1  | All | All | All |
| Application | IBM | Java | 6.0.9.2  | All | All | All |
| Application | IBM | Java | 7.0.0.0  | All | All | All |
| Application | IBM | Java | 7.0.1.0  | All | All | All |
| Application | IBM | Java | 7.0.2.0  | All | All | All |
| Application | IBM | Java | 7.0.3.0  | All | All | All |

|                                           |             |              |         |     |     |     |
|-------------------------------------------|-------------|--------------|---------|-----|-----|-----|
| Application                               | l <b>bm</b> | J <b>ava</b> | 7.0.4.0 | All | All | All |
| Application                               | l <b>bm</b> | J <b>ava</b> | 7.0.4.1 | All | All | All |
| Application                               | l <b>bm</b> | J <b>ava</b> | 7.0.4.2 | All | All | All |
| cpe:2.3:a:ibm:java:1.4.2:*:*:*:*:*:       |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13:*:*:*:*:*:    |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.1:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.10:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.11:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.12:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.13:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.14:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.15:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.16:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.17:*:*:*:*:*: |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.2:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.3:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.4:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.5:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.6:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.7:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.8:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:1.4.2.13.9:*:*:*:*:*:  |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.0.0:*:*:*:*:*:     |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.11.0:*:*:*:*:*:    |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.11.1:*:*:*:*:*:    |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.11.2:*:*:*:*:*:    |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.12.0:*:*:*:*:*:    |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.12.1:*:*:*:*:*:    |             |              |         |     |     |     |
| cpe:2.3:a:ibm:java:5.0.12.2:*:*:*:*:*:    |             |              |         |     |     |     |

|                                    |
|------------------------------------|
| cpe:2.3:a:ibm:java:5.0.12.3:*****: |
| cpe:2.3:a:ibm:java:5.0.12.4:*****: |
| cpe:2.3:a:ibm:java:5.0.12.5:*****: |
| cpe:2.3:a:ibm:java:5.0.13.0:*****: |
| cpe:2.3:a:ibm:java:5.0.14.0:*****: |
| cpe:2.3:a:ibm:java:5.0.15.0:*****: |
| cpe:2.3:a:ibm:java:5.0.16.0:*****: |
| cpe:2.3:a:ibm:java:5.0.16.1:*****: |
| cpe:2.3:a:ibm:java:5.0.16.2:*****: |
| cpe:2.3:a:ibm:java:6.0.0.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.1.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.10.0:*****: |
| cpe:2.3:a:ibm:java:6.0.10.1:*****: |
| cpe:2.3:a:ibm:java:6.0.11.0:*****: |
| cpe:2.3:a:ibm:java:6.0.12.0:*****: |
| cpe:2.3:a:ibm:java:6.0.13.0:*****: |
| cpe:2.3:a:ibm:java:6.0.13.1:*****: |
| cpe:2.3:a:ibm:java:6.0.13.2:*****: |
| cpe:2.3:a:ibm:java:6.0.2.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.3.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.4.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.5.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.6.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.7.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.8.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.8.1:*****:  |
| cpe:2.3:a:ibm:java:6.0.9.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.9.1:*****:  |



|                                       |
|---------------------------------------|
| cpe:2.3:a:ibm:java:6.0.9.2:*****:     |
| cpe:2.3:a:ibm:java:7.0.0.0:*****:     |
| cpe:2.3:a:ibm:java:7.0.1.0:*****:     |
| cpe:2.3:a:ibm:java:7.0.2.0:*****:     |
| cpe:2.3:a:ibm:java:7.0.3.0:*****:     |
| cpe:2.3:a:ibm:java:7.0.4.0:*****:     |
| cpe:2.3:a:ibm:java:7.0.4.1:*****:     |
| cpe:2.3:a:ibm:java:7.0.4.2:*****:     |
| cpe:2.3:a:ibm:java:1.4.2:*****:       |
| cpe:2.3:a:ibm:java:1.4.2.13:*****:    |
| cpe:2.3:a:ibm:java:1.4.2.13.1:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.10:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.11:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.12:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.13:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.14:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.15:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.16:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.17:*****: |
| cpe:2.3:a:ibm:java:1.4.2.13.2:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.3:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.4:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.5:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.6:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.7:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.8:*****:  |
| cpe:2.3:a:ibm:java:1.4.2.13.9:*****:  |
| cpe:2.3:a:ibm:java:5.0.0.0:*****:     |
| cpe:2.3:a:ibm:java:5.0.11.0:*****:    |

|                                    |
|------------------------------------|
|                                    |
| cpe:2.3:a:ibm:java:5.0.11.1:*****: |
| cpe:2.3:a:ibm:java:5.0.11.2:*****: |
| cpe:2.3:a:ibm:java:5.0.12.0:*****: |
| cpe:2.3:a:ibm:java:5.0.12.1:*****: |
| cpe:2.3:a:ibm:java:5.0.12.2:*****: |
| cpe:2.3:a:ibm:java:5.0.12.3:*****: |
| cpe:2.3:a:ibm:java:5.0.12.4:*****: |
| cpe:2.3:a:ibm:java:5.0.12.5:*****: |
| cpe:2.3:a:ibm:java:5.0.13.0:*****: |
| cpe:2.3:a:ibm:java:5.0.14.0:*****: |
| cpe:2.3:a:ibm:java:5.0.15.0:*****: |
| cpe:2.3:a:ibm:java:5.0.16.0:*****: |
| cpe:2.3:a:ibm:java:5.0.16.1:*****: |
| cpe:2.3:a:ibm:java:5.0.16.2:*****: |
| cpe:2.3:a:ibm:java:6.0.0.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.1.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.10.0:*****: |
| cpe:2.3:a:ibm:java:6.0.10.1:*****: |
| cpe:2.3:a:ibm:java:6.0.11.0:*****: |
| cpe:2.3:a:ibm:java:6.0.12.0:*****: |
| cpe:2.3:a:ibm:java:6.0.13.0:*****: |
| cpe:2.3:a:ibm:java:6.0.13.1:*****: |
| cpe:2.3:a:ibm:java:6.0.13.2:*****: |
| cpe:2.3:a:ibm:java:6.0.2.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.3.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.4.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.5.0:*****:  |
| cpe:2.3:a:ibm:java:6.0.6.0:*****:  |
|                                    |

|                                   |
|-----------------------------------|
| cpe:2.3:a:ibm:java:6.0.7.0:*****: |
| cpe:2.3:a:ibm:java:6.0.8.0:*****: |
| cpe:2.3:a:ibm:java:6.0.8.1:*****: |
| cpe:2.3:a:ibm:java:6.0.9.0:*****: |
| cpe:2.3:a:ibm:java:6.0.9.1:*****: |
| cpe:2.3:a:ibm:java:6.0.9.2:*****: |
| cpe:2.3:a:ibm:java:7.0.0.0:*****: |
| cpe:2.3:a:ibm:java:7.0.1.0:*****: |
| cpe:2.3:a:ibm:java:7.0.2.0:*****: |
| cpe:2.3:a:ibm:java:7.0.3.0:*****: |
| cpe:2.3:a:ibm:java:7.0.4.0:*****: |
| cpe:2.3:a:ibm:java:7.0.4.1:*****: |
| cpe:2.3:a:ibm:java:7.0.4.2:*****: |

No vendor comments have been submitted for this CVE

[← 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](#)