



Published on: 01/14/2012 12:00:00 AM UTC

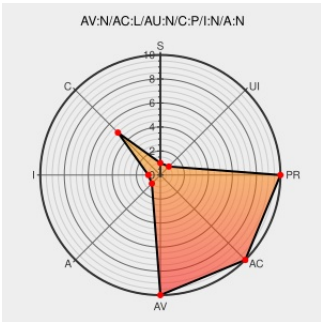
Last Modified on: 02/13/2023 12:15:00 AM UTC

CVE-2011-1184

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Tomcat](#) from [Apache](#) contain the following vulnerability:



The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nc (aka nonce-count or client nonce count) values.

CVE-2011-1184 has been assigned by  secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20190319 svn commit: r1855831 [22/30] - in /tomcat/site/trunk: ./ docs/ xdocs/
'[security bulletin] HPSBUX02860 SSRT101146 rev.1 - HP-UX Apache Running Tomcat Servlet Engine, Remot' - MARC	marc.info text/html	 HP HPSBUX02860
Debian -- Security Information -- DSA-2401-1 tomcat6	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2401
About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 57126

text/plain

Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20200203 svn commit: r1873527 [22/30] - /tomcat/site/trunk/docs/
Red Hat Customer Portal	www.redhat.com text/html	 REDHAT RHSA-2011:1845
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0077
[security-announce] openSUSE-SU-2012:0208-1: important: tomcat6: Fix mul	lists.opensuse.org text/html	 SUSE openSUSE-SU-2012:0208
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0325
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:19169
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0075
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0076
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20200213 svn commit: r1873980 [25/34] - /tomcat/site/trunk/docs/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0078
Apache Tomcat - Apache Tomcat 5 vulnerabilities	Vendor Advisory tomcat.apache.org text/html	 CONFIRM tomcat.apache.org/security-5.html
mandriva.com	www.mandriva.com text/html	 MANDRIVA MDVSA-2011:156
[Apache-SVN] Revision 1159309	Patch svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=rev&rev=1159309
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20190325 svn commit: r1856174 [20/29] - in /tomcat/site/trunk: docs/ xdocs/ xdocs/stylesheets/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:0074
Apache Tomcat® - Apache Tomcat 7 vulnerabilities	Vendor Advisory tomcat.apache.org text/html	 CONFIRM tomcat.apache.org/security-7.html
[Apache-SVN] Revision 1087655	Patch svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=rev&rev=1087655
[security-announce] SUSE-SU-2012:0155-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2012:0155
'[security bulletin] HPSBOV02762 SSRT100825 rev.1 - HP Secure Web Server (SWS) for OpenVMS running CS' -	marc.info text/html	 HP HPSBOV02762

MARC

'[security bulletin] HPSBST02955 rev.1 - HP XP P9000 Performance Advisor Software, 3rd party Software' - MARC

[marc.info](#)
[text/html](#)
 [HP HPSBST02955](#)

[Apache-SVN] Revision 1158180

[Patch](#)
[svn.apache.org](#)
[text/html](#)
 [CONFIRM svn.apache.org/viewvc?view=rev&rev=1158180](#)

Apache Tomcat® - Apache Tomcat 6 vulnerabilities

[Vendor Advisory](#)
[tomcat.apache.org](#)
[text/html](#)
 [CONFIRM tomcat.apache.org/security-6.html](#)

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	Apache	Tomcat	5.5.0	All	All	All
Application	Apache	Tomcat	5.5.1	All	All	All
Application	Apache	Tomcat	5.5.10	All	All	All
Application	Apache	Tomcat	5.5.11	All	All	All
Application	Apache	Tomcat	5.5.12	All	All	All
Application	Apache	Tomcat	5.5.13	All	All	All
Application	Apache	Tomcat	5.5.14	All	All	All
Application	Apache	Tomcat	5.5.15	All	All	All
Application	Apache	Tomcat	5.5.16	All	All	All
Application	Apache	Tomcat	5.5.17	All	All	All
Application	Apache	Tomcat	5.5.18	All	All	All
Application	Apache	Tomcat	5.5.19	All	All	All
Application	Apache	Tomcat	5.5.2	All	All	All
Application	Apache	Tomcat	5.5.20	All	All	All
Application	Apache	Tomcat	5.5.21	All	All	All
Application	Apache	Tomcat	5.5.22	All	All	All
Application	Apache	Tomcat	5.5.23	All	All	All
Application	Apache	Tomcat	5.5.24	All	All	All
Application	Apache	Tomcat	5.5.25	All	All	All
Application	Apache	Tomcat	5.5.26	All	All	All
Application	Apache	Tomcat	5.5.27	All	All	All

Application	Apache	Tomcat	5.5.28	All	All	All
Application	Apache	Tomcat	5.5.29	All	All	All
Application	Apache	Tomcat	5.5.3	All	All	All
Application	Apache	Tomcat	5.5.30	All	All	All
Application	Apache	Tomcat	5.5.31	All	All	All
Application	Apache	Tomcat	5.5.32	All	All	All
Application	Apache	Tomcat	5.5.33	All	All	All
Application	Apache	Tomcat	5.5.4	All	All	All
Application	Apache	Tomcat	5.5.5	All	All	All
Application	Apache	Tomcat	5.5.6	All	All	All
Application	Apache	Tomcat	5.5.7	All	All	All
Application	Apache	Tomcat	5.5.8	All	All	All
Application	Apache	Tomcat	5.5.9	All	All	All
Application	Apache	Tomcat	6.0	All	All	All
Application	Apache	Tomcat	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.10	All	All	All
Application	Apache	Tomcat	6.0.11	All	All	All
Application	Apache	Tomcat	6.0.12	All	All	All
Application	Apache	Tomcat	6.0.13	All	All	All
Application	Apache	Tomcat	6.0.14	All	All	All
Application	Apache	Tomcat	6.0.15	All	All	All
Application	Apache	Tomcat	6.0.16	All	All	All
Application	Apache	Tomcat	6.0.17	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All
Application	Apache	Tomcat	6.0.19	All	All	All
Application	Apache	Tomcat	6.0.2	All	All	All
Application	Apache	Tomcat	6.0.20	All	All	All
Application	Apache	Tomcat	6.0.24	All	All	All
Application	Apache	Tomcat	6.0.26	All	All	All
Application	Apache	Tomcat	6.0.27	All	All	All
Application	Apache	Tomcat	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	6.0.3	All	All	All
Application	Apache	Tomcat	6.0.30	All	All	All

Application	Apache	Tomcat	6.0.31	All	All	All
Application	Apache	Tomcat	6.0.32	All	All	All
Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.5	All	All	All
Application	Apache	Tomcat	6.0.6	All	All	All
Application	Apache	Tomcat	6.0.7	All	All	All
Application	Apache	Tomcat	6.0.8	All	All	All
Application	Apache	Tomcat	6.0.9	All	All	All
Application	Apache	Tomcat	7.0.0	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.1	All	All	All
Application	Apache	Tomcat	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All
Application	Apache	Tomcat	7.0.5	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.7	All	All	All
Application	Apache	Tomcat	7.0.8	All	All	All
Application	Apache	Tomcat	7.0.9	All	All	All
Application	Apache	Tomcat	5.5.0	All	All	All
Application	Apache	Tomcat	5.5.1	All	All	All
Application	Apache	Tomcat	5.5.10	All	All	All
Application	Apache	Tomcat	5.5.11	All	All	All
Application	Apache	Tomcat	5.5.12	All	All	All
Application	Apache	Tomcat	5.5.13	All	All	All
Application	Apache	Tomcat	5.5.14	All	All	All
Application	Apache	Tomcat	5.5.15	All	All	All
Application	Apache	Tomcat	5.5.16	All	All	All
Application	Apache	Tomcat	5.5.17	All	All	All
Application	Apache	Tomcat	5.5.18	All	All	All
Application	Apache	Tomcat	5.5.19	All	All	All
Application	Apache	Tomcat	5.5.2	All	All	All
Application	Apache	Tomcat	5.5.20	All	All	All
Application	Apache	Tomcat	5.5.21	All	All	All

Application	Apache	Tomcat	5.5.22	All	All	All
Application	Apache	Tomcat	5.5.23	All	All	All
Application	Apache	Tomcat	5.5.24	All	All	All
Application	Apache	Tomcat	5.5.25	All	All	All
Application	Apache	Tomcat	5.5.26	All	All	All
Application	Apache	Tomcat	5.5.27	All	All	All
Application	Apache	Tomcat	5.5.28	All	All	All
Application	Apache	Tomcat	5.5.29	All	All	All
Application	Apache	Tomcat	5.5.3	All	All	All
Application	Apache	Tomcat	5.5.30	All	All	All
Application	Apache	Tomcat	5.5.31	All	All	All
Application	Apache	Tomcat	5.5.32	All	All	All
Application	Apache	Tomcat	5.5.33	All	All	All
Application	Apache	Tomcat	5.5.4	All	All	All
Application	Apache	Tomcat	5.5.5	All	All	All
Application	Apache	Tomcat	5.5.6	All	All	All
Application	Apache	Tomcat	5.5.7	All	All	All
Application	Apache	Tomcat	5.5.8	All	All	All
Application	Apache	Tomcat	5.5.9	All	All	All
Application	Apache	Tomcat	6.0	All	All	All
Application	Apache	Tomcat	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.10	All	All	All
Application	Apache	Tomcat	6.0.11	All	All	All
Application	Apache	Tomcat	6.0.12	All	All	All
Application	Apache	Tomcat	6.0.13	All	All	All
Application	Apache	Tomcat	6.0.14	All	All	All
Application	Apache	Tomcat	6.0.15	All	All	All
Application	Apache	Tomcat	6.0.16	All	All	All
Application	Apache	Tomcat	6.0.17	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All
Application	Apache	Tomcat	6.0.19	All	All	All
Application	Apache	Tomcat	6.0.2	All	All	All
Application	Apache	Tomcat	6.0.20	All	All	All
Application	Apache	Tomcat	6.0.24	All	All	All

Application	Apache	Tomcat	6.0.26	All	All	All
Application	Apache	Tomcat	6.0.27	All	All	All
Application	Apache	Tomcat	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	6.0.3	All	All	All
Application	Apache	Tomcat	6.0.30	All	All	All
Application	Apache	Tomcat	6.0.31	All	All	All
Application	Apache	Tomcat	6.0.32	All	All	All
Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.5	All	All	All
Application	Apache	Tomcat	6.0.6	All	All	All
Application	Apache	Tomcat	6.0.7	All	All	All
Application	Apache	Tomcat	6.0.8	All	All	All
Application	Apache	Tomcat	6.0.9	All	All	All
Application	Apache	Tomcat	7.0.0	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.1	All	All	All
Application	Apache	Tomcat	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.2	All	All	All
Application	Apache	Tomcat	7.0.3	All	All	All
Application	Apache	Tomcat	7.0.4	All	All	All
Application	Apache	Tomcat	7.0.5	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.7	All	All	All
Application	Apache	Tomcat	7.0.8	All	All	All
Application	Apache	Tomcat	7.0.9	All	All	All
cpe:2.3:a:apache:tomcat:5.5.0:*****:*						
cpe:2.3:a:apache:tomcat:5.5.1:*****:*						
cpe:2.3:a:apache:tomcat:5.5.10:*****:*						
cpe:2.3:a:apache:tomcat:5.5.11:*****:*						
cpe:2.3:a:apache:tomcat:5.5.12:*****:*						
cpe:2.3:a:apache:tomcat:5.5.13:*****:*						
cpe:2.3:a:apache:tomcat:5.5.14:*****:*						

```
cpe:2.3:a:apache:tomcat:5.5.15:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.16:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.17:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.18:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.19:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.20:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.21:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.22:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.23:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.24:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.25:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.26:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.27:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.28:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.29:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.30:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.31:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:apache:tomcat:5.5.32:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.33:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.5:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:5.5.9:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:apache:tomcat:6.0:*:*:*:*:*:
```

cpe:2.3:a:apache:tomcat:6.0.0:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.1:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.10:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.11:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.12:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.13:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.14:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.15:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.16:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.17:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.18:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.19:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.2:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.20:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.24:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.26:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.27:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.28:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.29:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.3:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.30:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.31:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.32:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.4:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.5:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.6:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.7:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.8:****:*:*:
cpe:2.3:a:apache:tomcat:6.0.9:****:*:*:

cpe:2.3:a:apache:tomcat:7.0.0:*****:
cpe:2.3:a:apache:tomcat:7.0.0:beta:*****:
cpe:2.3:a:apache:tomcat:7.0.1:*****:
cpe:2.3:a:apache:tomcat:7.0.10:*****:
cpe:2.3:a:apache:tomcat:7.0.11:*****:
cpe:2.3:a:apache:tomcat:7.0.2:*****:
cpe:2.3:a:apache:tomcat:7.0.3:*****:
cpe:2.3:a:apache:tomcat:7.0.4:*****:
cpe:2.3:a:apache:tomcat:7.0.5:*****:
cpe:2.3:a:apache:tomcat:7.0.6:*****:
cpe:2.3:a:apache:tomcat:7.0.7:*****:
cpe:2.3:a:apache:tomcat:7.0.8:*****:
cpe:2.3:a:apache:tomcat:7.0.9:*****:
cpe:2.3:a:apache:tomcat:5.5.0:*****:
cpe:2.3:a:apache:tomcat:5.5.1:*****:
cpe:2.3:a:apache:tomcat:5.5.10:*****:
cpe:2.3:a:apache:tomcat:5.5.11:*****:
cpe:2.3:a:apache:tomcat:5.5.12:*****:
cpe:2.3:a:apache:tomcat:5.5.13:*****:
cpe:2.3:a:apache:tomcat:5.5.14:*****:
cpe:2.3:a:apache:tomcat:5.5.15:*****:
cpe:2.3:a:apache:tomcat:5.5.16:*****:
cpe:2.3:a:apache:tomcat:5.5.17:*****:
cpe:2.3:a:apache:tomcat:5.5.18:*****:
cpe:2.3:a:apache:tomcat:5.5.19:*****:
cpe:2.3:a:apache:tomcat:5.5.2:*****:
cpe:2.3:a:apache:tomcat:5.5.20:*****:
cpe:2.3:a:apache:tomcat:5.5.21:*****:

cpe:2.3:a:apache:tomcat:5.5.22:*****:
cpe:2.3:a:apache:tomcat:5.5.23:*****:
cpe:2.3:a:apache:tomcat:5.5.24:*****:
cpe:2.3:a:apache:tomcat:5.5.25:*****:
cpe:2.3:a:apache:tomcat:5.5.26:*****:
cpe:2.3:a:apache:tomcat:5.5.27:*****:
cpe:2.3:a:apache:tomcat:5.5.28:*****:
cpe:2.3:a:apache:tomcat:5.5.29:*****:
cpe:2.3:a:apache:tomcat:5.5.3:*****:
cpe:2.3:a:apache:tomcat:5.5.30:*****:
cpe:2.3:a:apache:tomcat:5.5.31:*****:
cpe:2.3:a:apache:tomcat:5.5.32:*****:
cpe:2.3:a:apache:tomcat:5.5.33:*****:
cpe:2.3:a:apache:tomcat:5.5.4:*****:
cpe:2.3:a:apache:tomcat:5.5.5:*****:
cpe:2.3:a:apache:tomcat:5.5.6:*****:
cpe:2.3:a:apache:tomcat:5.5.7:*****:
cpe:2.3:a:apache:tomcat:5.5.8:*****:
cpe:2.3:a:apache:tomcat:5.5.9:*****:
cpe:2.3:a:apache:tomcat:6.0:*****:
cpe:2.3:a:apache:tomcat:6.0.0:*****:
cpe:2.3:a:apache:tomcat:6.0.1:*****:
cpe:2.3:a:apache:tomcat:6.0.10:*****:
cpe:2.3:a:apache:tomcat:6.0.11:*****:
cpe:2.3:a:apache:tomcat:6.0.12:*****:
cpe:2.3:a:apache:tomcat:6.0.13:*****:
cpe:2.3:a:apache:tomcat:6.0.14:*****:
cpe:2.3:a:apache:tomcat:6.0.15:*****:
cpe:2.3:a:apache:tomcat:6.0.16:*****:

```
cpe:2.3:a:apache:tomcat:b.0.16:::~::~
```

```
cpe:2.3:a:apache:tomcat:6.0.17:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.18:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.19:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.20:::*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.24:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.26:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.27:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.28:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.29:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.3:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.30:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:apache:tomcat:6.0.31:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:apache:tomcat:6.0.32:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.0:beta:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.11:::*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.4:*:*:*:*:*:*:
```

cpe:2.3:a:apache:tomcat:7.0.5:*****:
cpe:2.3:a:apache:tomcat:7.0.6:*****:
cpe:2.3:a:apache:tomcat:7.0.7:*****:
cpe:2.3:a:apache:tomcat:7.0.8:*****:
cpe:2.3:a:apache:tomcat:7.0.9:*****:

No vendor comments have been submitted for this CVE

← Previous IDNext 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](#)