



CVE-2015-5345

Published on: 02/24/2016 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:26:00 AM UTC

CVE-2015-5345

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



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

The Mapper component in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.30, and 9.x before 9.0.0.M2 processes redirects before considering security constraints and Filters, which allows remote attackers to determine the existence of a directory via a URL that lacks a trailing / (slash) character.

CVE-2015-5345 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	LOW	NONE	NONE

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] 20190413 svn commit: r1857494 [15/20] - in /tomcat/site/trunk: ./ docs/ xdocs/
Oracle Solaris Bulletin - April 2016	www.oracle.com	CONFIRM

Oracle Security Bulletin - April 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html
'[security bulletin] HPSBUX03561 rev.1 - HPE HP-UX using Apache Tomcat, Remote Access Restriction Byp' - MARC	marc.info text/html	 HP HPSBUX03561
[Apache-SVN] Revision 1715206	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1715206
CVE-2015-5345: Information disclosure vulnerability in Apache Tomcat - Security Blog - QCSec	www.qcsec.com text/html	 MISC www.qcsec.com/blog/CVE-2015-5345-apache-tomcat-vulnerability.html
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20190415 svn commit: r1857582 [16/22] - in /tomcat/site/trunk: docs/ xdocs/stylesheets/
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20190325 svn commit: r1856174 [21/29] - in /tomcat/site/trunk: docs/ xdocs/ xdocs/stylesheets/
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20200213 svn commit: r1873980 [27/34] - /tomcat/site/trunk/docs/
Apache Tomcat Flaw Lets Remote Users Determine Valid Directories - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1035071
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20200203 svn commit: r1873527 [23/30] - /tomcat/site/trunk/docs/
[Apache-SVN] Revision 1715213	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1715213
[Apache-SVN] Revision 1716882	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1716882
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20190319 svn commit: r1855831 [23/30] - in /tomcat/site/trunk: ./ docs/ xdocs/
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2045
Full Disclosure: [CVE-2015-5345] Information disclosure vulnerability in Apache Tomcat	seclists.org text/html	 FULLDISC 20160225 [CVE-2015-5345] Information disclosure vulnerability in Apache Tomcat
Debian -- Security Information -- DSA-3609-1 tomcat8	www.debian.org text/html Deprecated Link	 DEBIAN DSA-3609
CPU July 2018	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
[security-announce] SUSE-SU-2016:0769-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0769
Oracle Linux Bulletin - October 2016	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinoct2016-3090545.html
[security-announce] SUSE-SU-2016:0822-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0822
[Apache-SVN] Revision 1716894	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1716894
[security-announce] openSUSE-SU-	lists.opensuse.org	 SUSE openSUSE-SU-2016:0865

2016:0865-1: important: Security update	text/html	
February 2016 Apache Tomcat Vulnerabilities in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20180531-0001/
Apache Tomcat Directory Disclosure ~ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/135892/Apache-Tomcat-Directory-Disclosure.html
Pony Mail!	lists.apache.org text/html	 MLIST [tomcat-dev] 20200213 svn commit: r1873980 [26/34] - /tomcat/site/trunk/docs/
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2016:1087
Document Display HPE Support Center	h20566.www2.hpe.com text/html	 CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158626
Document Display HPE Support Center	h20566.www2.hpe.com text/html	 CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05150442
[Apache-SVN] Revision 1717209	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1717209
Bugtraq: [SECURITY] CVE-2015-5345 Apache Tomcat Directory disclosure	seclists.org text/html	 BUGTRAQ 20160222 [SECURITY] CVE-2015-5345 Apache Tomcat Directory disclosure
USN-3024-1: Tomcat vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-3024-1
[Apache-SVN] Revision 1717212	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1717212
Debian -- Security Information -- DSA-3530-1 tomcat6	www.debian.org text/html Deprecated Link	 DEBIAN DSA-3530
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:2599
No Description Provided	rhn.redhat.com Inactive Link Not Archived	 REDHAT RHSA-2016:1089
Broadcom Support Portal	bto.bluecoat.com text/html	 CONFIRM bto.bluecoat.com/security-advisory/sa118
Document Display HPE Support Center	h20566.www2.hpe.com text/html	 CONFIRM h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05054964
[Apache-SVN] Revision 1715216	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1715216
[security-announce] SUSE-SU-2016:0839-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2016:0839
McAfee Security Bulletin: McAfee Web Gateway update fixes multiple vulnerabilities	kc.mcafee.com text/html	 CONFIRM kc.mcafee.com/corporate/index?page=content&id=SB10156
Apache Tomcat® - Apache Tomcat 7 vulnerabilities	Vendor Advisory tomcat.apache.org text/html	 CONFIRM tomcat.apache.org/security-7.html
Apache Tomcat® - Apache Tomcat 8 vulnerabilities	Vendor Advisory tomcat.apache.org text/html	 CONFIRM tomcat.apache.org/security-8.html

Apache Tomcat® - Apache Tomcat 8 vulnerabilities	Vendor Advisory tomcat.apache.org text/html	 CONFIRM tomcat.apache.org/security-8.html
[Apache-SVN] Revision 1717216	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1717216
Apache Tomcat: Multiple vulnerabilities (GLSA 201705-09) — Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201705-09
Bug 58765 – Default behavior change in tomcat 8.0.29-30 context root redirect process	bz.apache.org text/html	 CONFIRM bz.apache.org/bugzilla/show_bug.cgi?id=58765
Red Hat Customer Portal	access.redhat.com text/html	 REDHAT RHSA-2016:1088
[Apache-SVN] Revision 1715207	svn.apache.org text/html	 CONFIRM svn.apache.org/viewvc?view=revision&revision=1715207
Apache Tomcat CVE-2015-5345 Directory Traversal Vulnerability	cve.report (archive) text/html	 BID 83328
Apache Tomcat - Apache Tomcat 8 vulnerabilities	Vendor Advisory tomcat.apache.org text/html	 CONFIRM tomcat.apache.org/security-9.html
Debian -- Security Information -- DSA-3552-1 tomcat7	www.debian.org Deprecated Link text/html	 DEBIAN DSA-3552
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	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.0	alpha	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.1	alpha	All	All
Application	Apache	Tomcat	6.0.10	All	All	All
Application	Apache	Tomcat	6.0.11	All	All	All
Application	Apache	Tomcat	6.0.13	All	All	All
Application	Apache	Tomcat	6.0.14	All	All	All
Application	Apache	Tomcat	6.0.16	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All

Application	Apache	Tomcat	6.0.2	All	All	All
Application	Apache	Tomcat	6.0.2	alpha	All	All
Application	Apache	Tomcat	6.0.2	beta	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	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	6.0.30	All	All	All
Application	Apache	Tomcat	6.0.32	All	All	All
Application	Apache	Tomcat	6.0.33	All	All	All
Application	Apache	Tomcat	6.0.35	All	All	All
Application	Apache	Tomcat	6.0.36	All	All	All
Application	Apache	Tomcat	6.0.37	All	All	All
Application	Apache	Tomcat	6.0.39	All	All	All
Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.4	alpha	All	All
Application	Apache	Tomcat	6.0.41	All	All	All
Application	Apache	Tomcat	6.0.43	All	All	All
Application	Apache	Tomcat	6.0.44	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.12	All	All	All
Application	Apache	Tomcat	7.0.14	All	All	All
Application	Apache	Tomcat	7.0.16	All	All	All
Application	Apache	Tomcat	7.0.19	All	All	All
Application	Apache	Tomcat	7.0.2	beta	All	All
Application	Apache	Tomcat	7.0.20	All	All	All
Application	Apache	Tomcat	7.0.21	All	All	All
Application	Apache	Tomcat	7.0.22	All	All	All
Application	Apache	Tomcat	7.0.23	All	All	All
Application	Apache	Tomcat	7.0.25	All	All	All
Application	Apache	Tomcat	7.0.26	All	All	All
Application	Apache	Tomcat	7.0.27	All	All	All

Application	Apache	Tomcat	7.0.28	All	All	All
Application	Apache	Tomcat	7.0.29	All	All	All
Application	Apache	Tomcat	7.0.30	All	All	All
Application	Apache	Tomcat	7.0.32	All	All	All
Application	Apache	Tomcat	7.0.33	All	All	All
Application	Apache	Tomcat	7.0.34	All	All	All
Application	Apache	Tomcat	7.0.35	All	All	All
Application	Apache	Tomcat	7.0.37	All	All	All
Application	Apache	Tomcat	7.0.39	All	All	All
Application	Apache	Tomcat	7.0.4	beta	All	All
Application	Apache	Tomcat	7.0.40	All	All	All
Application	Apache	Tomcat	7.0.41	All	All	All
Application	Apache	Tomcat	7.0.42	All	All	All
Application	Apache	Tomcat	7.0.47	All	All	All
Application	Apache	Tomcat	7.0.5	beta	All	All
Application	Apache	Tomcat	7.0.50	All	All	All
Application	Apache	Tomcat	7.0.52	All	All	All
Application	Apache	Tomcat	7.0.53	All	All	All
Application	Apache	Tomcat	7.0.54	All	All	All
Application	Apache	Tomcat	7.0.55	All	All	All
Application	Apache	Tomcat	7.0.56	All	All	All
Application	Apache	Tomcat	7.0.57	All	All	All
Application	Apache	Tomcat	7.0.59	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.61	All	All	All
Application	Apache	Tomcat	7.0.62	All	All	All
Application	Apache	Tomcat	7.0.63	All	All	All
Application	Apache	Tomcat	7.0.64	All	All	All
Application	Apache	Tomcat	7.0.65	All	All	All
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc3	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.1	All	All	All
Application	Apache	Tomcat	8.0.11	All	All	All
Application	Apache	Tomcat	8.0.12	All	All	All

Application	Apache	Tomcat	Servlet	Java	Java	Java
Application	Apache	Tomcat	8.0.14	All	All	All
Application	Apache	Tomcat	8.0.15	All	All	All
Application	Apache	Tomcat	8.0.17	All	All	All
Application	Apache	Tomcat	8.0.18	All	All	All
Application	Apache	Tomcat	8.0.20	All	All	All
Application	Apache	Tomcat	8.0.21	All	All	All
Application	Apache	Tomcat	8.0.22	All	All	All
Application	Apache	Tomcat	8.0.23	All	All	All
Application	Apache	Tomcat	8.0.24	All	All	All
Application	Apache	Tomcat	8.0.26	All	All	All
Application	Apache	Tomcat	8.0.27	All	All	All
Application	Apache	Tomcat	8.0.28	All	All	All
Application	Apache	Tomcat	8.0.29	All	All	All
Application	Apache	Tomcat	8.0.3	All	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Application	Apache	Tomcat	6.0.0	All	All	All
Application	Apache	Tomcat	6.0.0	alpha	All	All
Application	Apache	Tomcat	6.0.1	All	All	All
Application	Apache	Tomcat	6.0.1	alpha	All	All
Application	Apache	Tomcat	6.0.10	All	All	All
Application	Apache	Tomcat	6.0.11	All	All	All
Application	Apache	Tomcat	6.0.13	All	All	All
Application	Apache	Tomcat	6.0.14	All	All	All
Application	Apache	Tomcat	6.0.16	All	All	All
Application	Apache	Tomcat	6.0.18	All	All	All
Application	Apache	Tomcat	6.0.2	All	All	All
Application	Apache	Tomcat	6.0.2	alpha	All	All
Application	Apache	Tomcat	6.0.2	beta	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	6.0.28	All	All	All
Application	Apache	Tomcat	6.0.29	All	All	All
Application	Apache	Tomcat	6.0.30	All	All	All
Application	Apache	Tomcat	6.0.32	All	All	All

Application	Apache	Tomcat	6.0.33	All	All	All
Application	Apache	Tomcat	6.0.35	All	All	All
Application	Apache	Tomcat	6.0.36	All	All	All
Application	Apache	Tomcat	6.0.37	All	All	All
Application	Apache	Tomcat	6.0.39	All	All	All
Application	Apache	Tomcat	6.0.4	All	All	All
Application	Apache	Tomcat	6.0.4	alpha	All	All
Application	Apache	Tomcat	6.0.41	All	All	All
Application	Apache	Tomcat	6.0.43	All	All	All
Application	Apache	Tomcat	6.0.44	All	All	All
Application	Apache	Tomcat	7.0.0	beta	All	All
Application	Apache	Tomcat	7.0.10	All	All	All
Application	Apache	Tomcat	7.0.11	All	All	All
Application	Apache	Tomcat	7.0.12	All	All	All
Application	Apache	Tomcat	7.0.14	All	All	All
Application	Apache	Tomcat	7.0.16	All	All	All
Application	Apache	Tomcat	7.0.19	All	All	All
Application	Apache	Tomcat	7.0.2	beta	All	All
Application	Apache	Tomcat	7.0.20	All	All	All
Application	Apache	Tomcat	7.0.21	All	All	All
Application	Apache	Tomcat	7.0.22	All	All	All
Application	Apache	Tomcat	7.0.23	All	All	All
Application	Apache	Tomcat	7.0.25	All	All	All
Application	Apache	Tomcat	7.0.26	All	All	All
Application	Apache	Tomcat	7.0.27	All	All	All
Application	Apache	Tomcat	7.0.28	All	All	All
Application	Apache	Tomcat	7.0.29	All	All	All
Application	Apache	Tomcat	7.0.30	All	All	All
Application	Apache	Tomcat	7.0.32	All	All	All
Application	Apache	Tomcat	7.0.33	All	All	All
Application	Apache	Tomcat	7.0.34	All	All	All
Application	Apache	Tomcat	7.0.35	All	All	All
Application	Apache	Tomcat	7.0.37	All	All	All
Application	Apache	Tomcat	7.0.39	All	All	All
Application	Apache	Tomcat	7.0.4	beta	All	All

Application	Apache	Tomcat	7.0.40	All	All	All
Application	Apache	Tomcat	7.0.41	All	All	All
Application	Apache	Tomcat	7.0.42	All	All	All
Application	Apache	Tomcat	7.0.47	All	All	All
Application	Apache	Tomcat	7.0.5	beta	All	All
Application	Apache	Tomcat	7.0.50	All	All	All
Application	Apache	Tomcat	7.0.52	All	All	All
Application	Apache	Tomcat	7.0.53	All	All	All
Application	Apache	Tomcat	7.0.54	All	All	All
Application	Apache	Tomcat	7.0.55	All	All	All
Application	Apache	Tomcat	7.0.56	All	All	All
Application	Apache	Tomcat	7.0.57	All	All	All
Application	Apache	Tomcat	7.0.59	All	All	All
Application	Apache	Tomcat	7.0.6	All	All	All
Application	Apache	Tomcat	7.0.61	All	All	All
Application	Apache	Tomcat	7.0.62	All	All	All
Application	Apache	Tomcat	7.0.63	All	All	All
Application	Apache	Tomcat	7.0.64	All	All	All
Application	Apache	Tomcat	7.0.65	All	All	All
Application	Apache	Tomcat	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc3	All	All
Application	Apache	Tomcat	8.0.0	rc5	All	All
Application	Apache	Tomcat	8.0.1	All	All	All
Application	Apache	Tomcat	8.0.11	All	All	All
Application	Apache	Tomcat	8.0.12	All	All	All
Application	Apache	Tomcat	8.0.14	All	All	All
Application	Apache	Tomcat	8.0.15	All	All	All
Application	Apache	Tomcat	8.0.17	All	All	All
Application	Apache	Tomcat	8.0.18	All	All	All
Application	Apache	Tomcat	8.0.20	All	All	All
Application	Apache	Tomcat	8.0.21	All	All	All
Application	Apache	Tomcat	8.0.22	All	All	All
Application	Apache	Tomcat	8.0.23	All	All	All
Application	Apache	Tomcat	8.0.24	All	All	All
Application	Apache	Tomcat	8.0.26	All	All	All

Application	Apache	Tomcat	8.0.27	All	All	All
Application	Apache	Tomcat	8.0.28	All	All	All
Application	Apache	Tomcat	8.0.29	All	All	All
Application	Apache	Tomcat	8.0.3	All	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
cpe:2.3:a:apache:tomcat:6.0.0:*****:*						
cpe:2.3:a:apache:tomcat:6.0.0:alpha:*****:*						
cpe:2.3:a:apache:tomcat:6.0.1:*****:*						
cpe:2.3:a:apache:tomcat:6.0.1:alpha:*****:*						
cpe:2.3:a:apache:tomcat:6.0.10:*****:*						
cpe:2.3:a:apache:tomcat:6.0.11:*****:*						
cpe:2.3:a:apache:tomcat:6.0.13:*****:*						
cpe:2.3:a:apache:tomcat:6.0.14:*****:*						
cpe:2.3:a:apache:tomcat:6.0.16:*****:*						

cpe:2.3:a:apache:tomcat:6.0.18:*****:
cpe:2.3:a:apache:tomcat:6.0.2:*****:
cpe:2.3:a:apache:tomcat:6.0.2:alpha:*****:
cpe:2.3:a:apache:tomcat:6.0.2:beta:*****:
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:6.0.28:*****:
cpe:2.3:a:apache:tomcat:6.0.29:*****:
cpe:2.3:a:apache:tomcat:6.0.30:*****:
cpe:2.3:a:apache:tomcat:6.0.32:*****:
cpe:2.3:a:apache:tomcat:6.0.33:*****:
cpe:2.3:a:apache:tomcat:6.0.35:*****:
cpe:2.3:a:apache:tomcat:6.0.36:*****:
cpe:2.3:a:apache:tomcat:6.0.37:*****:
cpe:2.3:a:apache:tomcat:6.0.39:*****:
cpe:2.3:a:apache:tomcat:6.0.4:*****:
cpe:2.3:a:apache:tomcat:6.0.4:alpha:*****:
cpe:2.3:a:apache:tomcat:6.0.41:*****:
cpe:2.3:a:apache:tomcat:6.0.43:*****:
cpe:2.3:a:apache:tomcat:6.0.44:*****:
cpe:2.3:a:apache:tomcat:7.0.0:beta:*****:
cpe:2.3:a:apache:tomcat:7.0.10:*****:
cpe:2.3:a:apache:tomcat:7.0.11:*****:
cpe:2.3:a:apache:tomcat:7.0.12:*****:
cpe:2.3:a:apache:tomcat:7.0.14:*****:
cpe:2.3:a:apache:tomcat:7.0.16:*****:
cpe:2.3:a:apache:tomcat:7.0.19:*****:
cpe:2.3:a:apache:tomcat:7.0.2:beta:*****:

cpe:2.3:a:apache:tomcat:7.0.20:*****:
cpe:2.3:a:apache:tomcat:7.0.21:*****:
cpe:2.3:a:apache:tomcat:7.0.22:*****:
cpe:2.3:a:apache:tomcat:7.0.23:*****:
cpe:2.3:a:apache:tomcat:7.0.25:*****:
cpe:2.3:a:apache:tomcat:7.0.26:*****:
cpe:2.3:a:apache:tomcat:7.0.27:*****:
cpe:2.3:a:apache:tomcat:7.0.28:*****:
cpe:2.3:a:apache:tomcat:7.0.29:*****:
cpe:2.3:a:apache:tomcat:7.0.30:*****:
cpe:2.3:a:apache:tomcat:7.0.32:*****:
cpe:2.3:a:apache:tomcat:7.0.33:*****:
cpe:2.3:a:apache:tomcat:7.0.34:*****:
cpe:2.3:a:apache:tomcat:7.0.35:*****:
cpe:2.3:a:apache:tomcat:7.0.37:*****:
cpe:2.3:a:apache:tomcat:7.0.39:*****:
cpe:2.3:a:apache:tomcat:7.0.4:beta:*****:
cpe:2.3:a:apache:tomcat:7.0.40:*****:
cpe:2.3:a:apache:tomcat:7.0.41:*****:
cpe:2.3:a:apache:tomcat:7.0.42:*****:
cpe:2.3:a:apache:tomcat:7.0.47:*****:
cpe:2.3:a:apache:tomcat:7.0.5:beta:*****:
cpe:2.3:a:apache:tomcat:7.0.50:*****:
cpe:2.3:a:apache:tomcat:7.0.52:*****:
cpe:2.3:a:apache:tomcat:7.0.53:*****:
cpe:2.3:a:apache:tomcat:7.0.54:*****:
cpe:2.3:a:apache:tomcat:7.0.55:*****:
cpe:2.3:a:apache:tomcat:7.0.56:*****:

```
cpe:2.3:a:apache:tomcat:7.0.57:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.59:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.61:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.62:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.63:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.64:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:7.0.65:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.0:rc1:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.0:rc10:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.0:rc3:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.0:rc5:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.11:::*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.12:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.14:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.15:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.17:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.18:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.20:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.21:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.22:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.23:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.24:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.26:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.27:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.28:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:8.0.29:*:*:*:*:*:*:
```

000-2 2:0:00choctomocut:2 0 2.*.*.*.*.*.*.

```

CPE.2.3.d.apache.tomcat.0.0.0 . . . . .

```

```
cpe:2.3:a:apache:tomcat:9.0.0:m1:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.0:alpha:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.1:alpha:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.10:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:apache:tomcat:6.0.11:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.13:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.14:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.16:*:*:*:*:*:*:
```

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

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

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

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

```
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:6.0.28:*:*:*:*:*:*:
```

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

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

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

```
cpe:2.3:a:apache:tomcat:6.0.33:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.35:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.36:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.37:*:*:*:*:*:*:
```

```
cpe:2.3:a:apache:tomcat:6.0.39:*:*:*:*:*:*:
```

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

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

cpe:2.3:a:apache:tomcat:6.0.41:~::~~::~~::
cpe:2.3:a:apache:tomcat:6.0.43:~::~~::~~::
cpe:2.3:a:apache:tomcat:6.0.44:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.0:beta:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.10:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.11:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.12:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.14:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.16:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.19:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.2:beta:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.20:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.21:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.22:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.23:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.25:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.26:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.27:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.28:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.29:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.30:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.32:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.33:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.34:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.35:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.37:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.39:~::~~::~~::
cpe:2.3:a:apache:tomcat:7.0.4:beta:~::~~::~~::

cpe:2.3:a:apache:tomcat:7.0.40:****:****:
cpe:2.3:a:apache:tomcat:7.0.41:****:****:
cpe:2.3:a:apache:tomcat:7.0.42:****:****:
cpe:2.3:a:apache:tomcat:7.0.47:****:****:
cpe:2.3:a:apache:tomcat:7.0.5:beta:****:****:
cpe:2.3:a:apache:tomcat:7.0.50:****:****:
cpe:2.3:a:apache:tomcat:7.0.52:****:****:
cpe:2.3:a:apache:tomcat:7.0.53:****:****:
cpe:2.3:a:apache:tomcat:7.0.54:****:****:
cpe:2.3:a:apache:tomcat:7.0.55:****:****:
cpe:2.3:a:apache:tomcat:7.0.56:****:****:
cpe:2.3:a:apache:tomcat:7.0.57:****:****:
cpe:2.3:a:apache:tomcat:7.0.59:****:****:
cpe:2.3:a:apache:tomcat:7.0.6:****:****:
cpe:2.3:a:apache:tomcat:7.0.61:****:****:
cpe:2.3:a:apache:tomcat:7.0.62:****:****:
cpe:2.3:a:apache:tomcat:7.0.63:****:****:
cpe:2.3:a:apache:tomcat:7.0.64:****:****:
cpe:2.3:a:apache:tomcat:7.0.65:****:****:
cpe:2.3:a:apache:tomcat:8.0.0:rc1:****:****:
cpe:2.3:a:apache:tomcat:8.0.0:rc10:****:****:
cpe:2.3:a:apache:tomcat:8.0.0:rc3:****:****:
cpe:2.3:a:apache:tomcat:8.0.0:rc5:****:****:
cpe:2.3:a:apache:tomcat:8.0.1:****:****:
cpe:2.3:a:apache:tomcat:8.0.11:****:****:
cpe:2.3:a:apache:tomcat:8.0.12:****:****:
cpe:2.3:a:apache:tomcat:8.0.14:****:****:
cpe:2.3:a:apache:tomcat:8.0.15:****:****:
cpe:2.3:a:apache:tomcat:8.0.17:****:****:

cpe:2.3:a:apache:tomcat:8.0.18:*****:
cpe:2.3:a:apache:tomcat:8.0.20:*****:
cpe:2.3:a:apache:tomcat:8.0.21:*****:
cpe:2.3:a:apache:tomcat:8.0.22:*****:
cpe:2.3:a:apache:tomcat:8.0.23:*****:
cpe:2.3:a:apache:tomcat:8.0.24:*****:
cpe:2.3:a:apache:tomcat:8.0.26:*****:
cpe:2.3:a:apache:tomcat:8.0.27:*****:
cpe:2.3:a:apache:tomcat:8.0.28:*****:
cpe:2.3:a:apache:tomcat:8.0.29:*****:
cpe:2.3:a:apache:tomcat:8.0.3:*****:
cpe:2.3:a:apache:tomcat:9.0.0:m1:*****:
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:
cpe:2.3:o:canonical:ubuntu_linux:15.10:*****:
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:lts:***:
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:lts:***:
cpe:2.3:o:canonical:ubuntu_linux:15.10:*****:
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:lts:***:
cpe:2.3:o:debian:debian_linux:7.0:*****:
cpe:2.3:o:debian:debian_linux:8.0:*****:
cpe:2.3:o:debian:debian_linux:7.0:*****:
cpe:2.3:o:debian:debian_linux:8.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)