



CVE-2014-7810

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-7810
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-06-07 23:59:03 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The Expression Language (EL) implementation in Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.58, and 8.x before 8.0.1

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:P/A:N

Problem Types: CWE-284 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:L/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

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	6.0.12	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	6.0.2	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	6.0.27	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	6.0.33	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	6.0.5	All	All	All

Application	Apache	Tomcat	6.0.6	All	All	All
Application	Apache	Tomcat	6.0.6	alpha	All	All
Application	Apache	Tomcat	6.0.7	All	All	All
Application	Apache	Tomcat	6.0.7	alpha	All	All
Application	Apache	Tomcat	6.0.7	beta	All	All
Application	Apache	Tomcat	6.0.8	All	All	All
Application	Apache	Tomcat	6.0.8	alpha	All	All
Application	Apache	Tomcat	6.0.9	All	All	All
Application	Apache	Tomcat	6.0.9	beta	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	7.0.12	All	All	All
Application	Apache	Tomcat	7.0.13	All	All	All
Application	Apache	Tomcat	7.0.14	All	All	All
Application	Apache	Tomcat	7.0.15	All	All	All
Application	Apache	Tomcat	7.0.16	All	All	All
Application	Apache	Tomcat	7.0.17	All	All	All
Application	Apache	Tomcat	7.0.18	All	All	All
Application	Apache	Tomcat	7.0.19	All	All	All
Application	Apache	Tomcat	7.0.2	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	7.0.24	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	7.0.3	All	All	All

Application	Apache	Tomcat	7.0.30	All	All	All
Application	Apache	Tomcat	7.0.31	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	7.0.36	All	All	All
Application	Apache	Tomcat	7.0.37	All	All	All
Application	Apache	Tomcat	7.0.38	All	All	All
Application	Apache	Tomcat	7.0.39	All	All	All
Application	Apache	Tomcat	7.0.4	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	7.0.43	All	All	All
Application	Apache	Tomcat	7.0.44	All	All	All
Application	Apache	Tomcat	7.0.45	All	All	All
Application	Apache	Tomcat	7.0.46	All	All	All
Application	Apache	Tomcat	7.0.47	All	All	All
Application	Apache	Tomcat	7.0.48	All	All	All
Application	Apache	Tomcat	7.0.49	All	All	All
Application	Apache	Tomcat	7.0.5	All	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	7.0.6	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	8.0.0	rc1	All	All
Application	Apache	Tomcat	8.0.0	rc2	All	All

Application	Apache	Tomcat	8.0.0	rc10	All	All
Application	Apache	Tomcat	8.0.0	rc2	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	8.0.3	All	All	All
Application	Apache	Tomcat	8.0.5	All	All	All
Application	Apache	Tomcat	8.0.8	All	All	All
Application	Apache	Tomcat	8.0.9	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference					Source	
USN-2654-1: Tomcat vulnerabilities Ubuntu					af854a3a-2127-422b	
Red Hat Customer Portal					af854a3a-2127-422b	
Apache Tomcat Security Manager Can Be Bypassed By Remote Users in Certain Cases - SecurityTracker					af854a3a-2127-422b	
Document Display HPE Support Center					af854a3a-2127-422b	
Debian -- Security Information -- DSA-3447-1 tomcat7					af854a3a-2127-422b	
Apache Tomcat® - Apache Tomcat 8 vulnerabilities					af854a3a-2127-422b	
'[security bulletin] HPSBUX03561 rev.1 - HPE HP-UX using Apache Tomcat, Remote Access Restriction Byp' - MARC					af854a3a-2127-422b	
Apache Tomcat® - Apache Tomcat 7 vulnerabilities					af854a3a-2127-422b	
Red Hat Customer Portal					af854a3a-2127-422b	
[Apache-SVN] Revision 1644018					af854a3a-2127-422b	
Debian -- Security Information -- DSA-3428-1 tomcat8					af854a3a-2127-422b	
Pony Mail!					af854a3a-2127-422b	
Oracle Solaris Third Party Bulletin - October 2015					af854a3a-2127-422b	
[Apache-SVN] Revision 1645642					af854a3a-2127-422b	
Pony Mail!					af854a3a-2127-422b	
Pony Mail!					af854a3a-2127-422b	
Pony Mail!					af854a3a-2127-422b	

Pony Mail!	af854a3a-2127-422b
Red Hat Customer Portal	af854a3a-2127-422b
USN-2655-1: Tomcat vulnerabilities Ubuntu	af854a3a-2127-422b
Pony Mail!	af854a3a-2127-422b
Oracle Linux Bulletin - October 2016	af854a3a-2127-422b
Apache Tomcat® - Apache Tomcat 6 vulnerabilities	af854a3a-2127-422b
Debian -- Security Information -- DSA-3530-1 tomcat6	af854a3a-2127-422b
CPU July 2018	af854a3a-2127-422b
Pony Mail!	af854a3a-2127-422b
Oracle Linux Bulletin - April 2016	af854a3a-2127-422b
Apache Tomcat CVE-2014-7810 Security Bypass Vulnerability	af854a3a-2127-422b
Red Hat Customer Portal	af854a3a-2127-422b
Pony Mail!	af854a3a-2127-422b
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
Pony Mail!	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)