



CVE-2015-5351

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

Summary

CVE	CVE-2015-5351
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-25 01:59:00 UTC
Updated	2023-12-08 16:41:00 UTC
Description	The (1) Manager and (2) Host Manager applications in Apache Tomcat 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	7.0.67	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	8.0.30	All	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Application	Apache	Tomcat	9.0.0	milestone1	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	7.0.30	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	7.0.67	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	8.0.30	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

References

Reference

Pony Mail!

Apache Tomcat CSRF Token Leak ~ Packet Storm

[Apache-SVN] Revision 1720661

Red Hat Customer Portal

Debian -- Security Information -- DSA-3609-1 tomcat8

[Apache-SVN] Revision 1720658

CPU July 2016
Pony Mail!
[security-announce] SUSE-SU-2016:0769-1: important: Security update for
[security-announce] SUSE-SU-2016:0822-1: important: Security update for
Oracle Critical Patch Update - October 2016
[security-announce] openSUSE-SU-2016:0865-1: important: Security update
February 2016 Apache Tomcat Vulnerabilities in NetApp Products NetApp Product Security
Red Hat Customer Portal
Document Display HPE Support Center
Document Display HPE Support Center
Red Hat Customer Portal
USN-3024-1: Tomcat vulnerabilities Ubuntu
Debian -- Security Information -- DSA-3530-1 tomcat6
Apache Tomcat CVE-2015-5351 Cross Site Request Forgery Vulnerability
Red Hat Customer Portal
[Apache-SVN] Revision 1720663
RHSA-2016:1089
Broadcom Support Portal
MySupport - Micro Focus Software Support
Bugtraq: [SECURITY] CVE-2015-5351 Apache Tomcat CSRF token leak
Apache Tomcat® - Apache Tomcat 7 vulnerabilities
Apache Tomcat® - Apache Tomcat 8 vulnerabilities
[Apache-SVN] Revision 1720655
Apache Tomcat Bugs Let Remote Users Bypass Security Restrictions, Hijack Sessions, and Obtain Potentially Sensitive Information - Security
Apache Tomcat: Multiple vulnerabilities (GLSA 201705-09) — Gentoo Security
[Apache-SVN] Revision 1720660
Red Hat Customer Portal
Oracle Critical Patch Update - October 2017
Apache Tomcat - Apache Tomcat 8 vulnerabilities
Debian -- Security Information -- DSA-3552-1 tomcat7
[Apache-SVN] Revision 1720652
CVE Program record
NVD vulnerability detail
◀ ▶

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

996880 Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-w7cg-5969-678w)

© [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](#).

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