



CVE-2016-0714

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2016-0714
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-25 01:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The session-persistence implementation in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.100 is vulnerable to a denial of service attack. An attacker can cause a denial of service by sending a request with a large session ID. The session ID is stored in memory and causes an out-of-memory error. This vulnerability affects Apache Tomcat versions 6.0.0 through 9.0.0.100.

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-264 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

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	6.0.13	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	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	milestone1	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

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

References
Reference
Document Display HPE Support Center
[security-announce] SUSE-SU-2016:0839-1: important: Security update for
[Apache-SVN] Revision 1726923
Document Display HPE Support Center
Red Hat Customer Portal
[Apache-SVN] Revision 1727182
USN-3024-1: Tomcat vulnerabilities Ubuntu
Oracle Critical Patch Update - October 2016
Debian -- Security Information -- DSA-3609-1 tomcat8
Apache Tomcat® - Apache Tomcat 8 vulnerabilities
[Apache-SVN] Revision 1727166
'[security bulletin] HPSBUX03561 rev.1 - HPE HP-UX using Apache Tomcat, Remote Access Restriction Byp' - MARC
Apache Tomcat® - Apache Tomcat 7 vulnerabilities

Debian -- Security Information -- DSA-3552-1 tomcat7
rhn.redhat.com/errata/RHSA-2016-1089.html
Red Hat Customer Portal
[security-announce] SUSE-SU-2016:0822-1: important: Security update for
[Apache-SVN] Revision 1726196
Pony Mail!
February 2016 Apache Tomcat Vulnerabilities in NetApp Products NetApp Product Security
Apache Tomcat Security Manager CVE-2016-0714 Remote Code Execution Vulnerability
[Apache-SVN] Revision 1726203
Oracle Critical Patch Update - October 2017
Bugtraq: [SECURITY] CVE-2016-0714 Apache Tomcat Security Manager Bypass
[security-announce] openSUSE-SU-2016:0865-1: important: Security update
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
Apache Tomcat: Multiple vulnerabilities (GLSA 201705-09) — Gentoo Security
Pony Mail!
Document Display HPE Support Center
Broadcom Support Portal
Pony Mail!
Oracle Linux Bulletin - October 2016
Apache Tomcat® - Apache Tomcat 6 vulnerabilities
[Apache-SVN] Revision 1725263
Red Hat Customer Portal
Debian -- Security Information -- DSA-3530-1 tomcat6
CPU July 2018
Pony Mail!
Apache Tomcat - Apache Tomcat 8 vulnerabilities
Red Hat Customer Portal
[security-announce] SUSE-SU-2016:0769-1: important: Security update for
MySQL Multiple Flaws Let Remote Authenticated and Local Users Access Data, Deny Service, and Gain Elevated Privileges - SecurityTracke
[Apache-SVN] Revision 1727034
Pony Mail!
Apache Tomcat Bugs Let Remote Users Bypass Security Restrictions, Hijack Sessions, and Obtain Potentially Sensitive Information - Security

Oracle Solaris Bulletin - April 2016
[Apache-SVN] Revision 1725914
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
CVE Program record
NVD vulnerability detail

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](#)