



CVE-2017-7675

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

Summary

CVE	CVE-2017-7675
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-11 02:29:00 UTC
Updated	2023-12-08 16:41:00 UTC
Description	The HTTP/2 implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M21 and 8.5.0 to 8.5.15 bypassed a number of security cl

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	8.5.0	All	All	All
Application	Apache	Tomcat	8.5.1	All	All	All
Application	Apache	Tomcat	8.5.10	All	All	All
Application	Apache	Tomcat	8.5.11	All	All	All
Application	Apache	Tomcat	8.5.12	All	All	All
Application	Apache	Tomcat	8.5.13	All	All	All
Application	Apache	Tomcat	8.5.14	All	All	All
Application	Apache	Tomcat	8.5.15	All	All	All
Application	Apache	Tomcat	8.5.2	All	All	All
Application	Apache	Tomcat	8.5.3	All	All	All
Application	Apache	Tomcat	8.5.4	All	All	All
Application	Apache	Tomcat	8.5.5	All	All	All
Application	Apache	Tomcat	8.5.6	All	All	All
Application	Apache	Tomcat	8.5.7	All	All	All
Application	Apache	Tomcat	8.5.8	All	All	All
Application	Apache	Tomcat	8.5.9	All	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All

Application	Apache	Tomcat	9.0.0	m10	All	All
Application	Apache	Tomcat	9.0.0	m11	All	All
Application	Apache	Tomcat	9.0.0	m12	All	All
Application	Apache	Tomcat	9.0.0	m13	All	All
Application	Apache	Tomcat	9.0.0	m14	All	All
Application	Apache	Tomcat	9.0.0	m15	All	All
Application	Apache	Tomcat	9.0.0	m16	All	All
Application	Apache	Tomcat	9.0.0	m17	All	All
Application	Apache	Tomcat	9.0.0	m18	All	All
Application	Apache	Tomcat	9.0.0	m19	All	All
Application	Apache	Tomcat	9.0.0	m2	All	All
Application	Apache	Tomcat	9.0.0	m20	All	All
Application	Apache	Tomcat	9.0.0	m21	All	All
Application	Apache	Tomcat	9.0.0	m3	All	All
Application	Apache	Tomcat	9.0.0	m4	All	All
Application	Apache	Tomcat	9.0.0	m5	All	All
Application	Apache	Tomcat	9.0.0	m6	All	All
Application	Apache	Tomcat	9.0.0	m7	All	All
Application	Apache	Tomcat	9.0.0	m8	All	All
Application	Apache	Tomcat	9.0.0	m9	All	All
Application	Apache	Tomcat	9.0.0	milestone1	All	All
Application	Apache	Tomcat	9.0.0	milestone10	All	All
Application	Apache	Tomcat	9.0.0	milestone11	All	All
Application	Apache	Tomcat	9.0.0	milestone12	All	All
Application	Apache	Tomcat	9.0.0	milestone13	All	All
Application	Apache	Tomcat	9.0.0	milestone14	All	All
Application	Apache	Tomcat	9.0.0	milestone15	All	All
Application	Apache	Tomcat	9.0.0	milestone16	All	All
Application	Apache	Tomcat	9.0.0	milestone17	All	All
Application	Apache	Tomcat	9.0.0	milestone18	All	All
Application	Apache	Tomcat	9.0.0	milestone19	All	All
Application	Apache	Tomcat	9.0.0	milestone2	All	All
Application	Apache	Tomcat	9.0.0	milestone20	All	All
Application	Apache	Tomcat	9.0.0	milestone21	All	All
Application	Apache	Tomcat	9.0.0	milestone3	All	All

Application	Apache	Tomcat	9.0.0	milestone4	All	All
Application	Apache	Tomcat	9.0.0	milestone5	All	All
Application	Apache	Tomcat	9.0.0	milestone6	All	All
Application	Apache	Tomcat	9.0.0	milestone7	All	All
Application	Apache	Tomcat	9.0.0	milestone8	All	All
Application	Apache	Tomcat	9.0.0	milestone9	All	All
Application	Apache	Tomcat	8.5.0	All	All	All
Application	Apache	Tomcat	8.5.1	All	All	All
Application	Apache	Tomcat	8.5.10	All	All	All
Application	Apache	Tomcat	8.5.11	All	All	All
Application	Apache	Tomcat	8.5.12	All	All	All
Application	Apache	Tomcat	8.5.13	All	All	All
Application	Apache	Tomcat	8.5.14	All	All	All
Application	Apache	Tomcat	8.5.15	All	All	All
Application	Apache	Tomcat	8.5.2	All	All	All
Application	Apache	Tomcat	8.5.3	All	All	All
Application	Apache	Tomcat	8.5.4	All	All	All
Application	Apache	Tomcat	8.5.5	All	All	All
Application	Apache	Tomcat	8.5.6	All	All	All
Application	Apache	Tomcat	8.5.7	All	All	All
Application	Apache	Tomcat	8.5.8	All	All	All
Application	Apache	Tomcat	8.5.9	All	All	All
Application	Apache	Tomcat	9.0.0	m1	All	All
Application	Apache	Tomcat	9.0.0	m10	All	All
Application	Apache	Tomcat	9.0.0	m11	All	All
Application	Apache	Tomcat	9.0.0	m12	All	All
Application	Apache	Tomcat	9.0.0	m13	All	All
Application	Apache	Tomcat	9.0.0	m14	All	All
Application	Apache	Tomcat	9.0.0	m15	All	All
Application	Apache	Tomcat	9.0.0	m16	All	All
Application	Apache	Tomcat	9.0.0	m17	All	All
Application	Apache	Tomcat	9.0.0	m18	All	All
Application	Apache	Tomcat	9.0.0	m19	All	All
Application	Apache	Tomcat	9.0.0	m2	All	All
Application	Apache	Tomcat	9.0.0	m20	All	All
Application	Apache	Tomcat	9.0.0	m3	All	All

Application	Apache	Tomcat	9.0.0	m21	All	All
Application	Apache	Tomcat	9.0.0	m3	All	All
Application	Apache	Tomcat	9.0.0	m4	All	All
Application	Apache	Tomcat	9.0.0	m5	All	All
Application	Apache	Tomcat	9.0.0	m6	All	All
Application	Apache	Tomcat	9.0.0	m7	All	All
Application	Apache	Tomcat	9.0.0	m8	All	All
Application	Apache	Tomcat	9.0.0	m9	All	All

References						
Reference	Source		Link	Tags		
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org	Mailing List, Vendor		
Pony Mail!	MLIST		lists.apache.org			
Apache Tomcat CVE-2017-7675 Directory Traversal Vulnerability	BID		www.securityfocus.com	Third Party Advisory		
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
Debian -- Security Information -- DSA-3974-1 tomcat8	DEBIAN		www.debian.org			
July 2017 Tomcat Vulnerabilities in NetApp Products NetApp Product Security	CONFIRM		security.netapp.com			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!			lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			
Pony Mail!	MLIST		lists.apache.org			

Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report