CVE-2019-17569

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

Summary

CVE	CVE-2019-17569
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-24 22:15:00 UTC
Updated	2023-11-07 03:06:00 UTC
Description	The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. T

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomee	7.0.7	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Netapp	Data Availability Services	-	All	All	All
Application	Netapp	Oncommand System Manager	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Oracle	Agile Engineering Data Management	6.2.1.0	All	All	All
Application	Oracle	Agile Plm	9.3.3	All	All	All
Application	Oracle	Agile Plm	9.3.5	All	All	All
Application	Oracle	Agile Plm	9.3.6	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.4.0	All	All	All
Application	Oracle	Health Sciences Empirica Inspections	1.0.1.2	All	All	All
Application	Oracle	Health Sciences Empirica Signal	7.3.3	All	All	All
Application	Oracle	Hospitality Guest Access	4.2.0	All	All	All

Application	Oracle	Hospitality Guest Access	4.2.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	All	All	All
Application	Oracle	Transportation Management	6.3.7	All	All	All
Application	Oracle	Workload Manager	12.2.0.1	All	All	All
Application	Oracle	Workload Manager	18c	All	All	All
Application	Oracle	Workload Manager	19c	All	All	All

References

Reference	Source	Link	Tags
February 2020 Apache Tomcat Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
Oracle Critical Patch Update Advisory - July 2020	MISC	www.oracle.com	
[SECURITY] [DLA 2133-1] tomcat7 security update	MLIST	lists.debian.org	Third Party
Oracle Critical Patch Update Advisory - October 2020	MISC	www.oracle.com	
Pony Mail!	MLIST	lists.apache.org	Mailing Lis
[security-announce] openSUSE-SU-2020:0345-1: important: Security update	SUSE	lists.opensuse.org	
Debian -- Security Information -- DSA-4673-1 tomcat8	DEBIAN	www.debian.org	
Pony Mail!		lists.apache.org	
Debian -- Security Information -- DSA-4680-1 tomcat9	DEBIAN	www.debian.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Oracle Critical Patch Update Advisory - January 2021	MISC	www.oracle.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

20277 Oracle Database 18c Critical OJVM Patch Update - July 2020

20281 Oracle Database 19c Critical OJVM Patch Update - July 2020

20292 Oracle Database 12.2.0.1 Critical OJVM Patch Update - July 2020

356190 Amazon Linux Security Advisory for tomcat : ALASTOMCAT8.5-2023-012

730112 Atlassian Jira Component Apache Tomcat Hypertext Transfer Protocol (HTTP) Request Smuggling Vulnerability (JRASERVER-70993)

730434 Update TITLE manually (JRASERVER-70487)

730441 Atlassian Jira Local Privilege Escalation Vulnerability (JRASERVER-70487)

730449 (JRASERVER-70487)

730510 Atlassian Jira Remote Code Execution (RCE) Vulnerability (JRASERVER-73223)

981583 Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-767j-jfh2-jvrc)

© 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 registred 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**