



# CVE-2019-12418

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-12418
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-23 18:15:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	When Apache Tomcat 9.0.0.M1 to 9.0.28, 8.5.0 to 8.5.47, 7.0.0 and 7.0.97 is configured with the JMX Remote Lifecycle Lis

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	All	All	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	All	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand System Manager</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Workload Manager</a>	12.2.0.1	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Workload Manager</a>	18c	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Workload Manager</a>	19c	All	All	All

## References

Reference	Source	Link	Tags
January 2020 Apache Tomcat Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	

Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Bugtraq: [SECURITY] [DSA 4596-1] tomcat8 security update	BUGTRAQ	<a href="https://seclists.org">seclists.org</a>	Mailing Lis
myF5		<a href="https://support.f5.com">support.f5.com</a>	
[SECURITY] [DLA 2155-1] tomcat8 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
<a href="https://support.f5.com/csp/article/K10107360">support.f5.com/csp/article/K10107360</a>	CONFIRM	<a href="https://support.f5.com">support.f5.com</a>	
[security-announce] openSUSE-SU-2020:0038-1: important: Security update	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Debian -- Security Information -- DSA-4596-1 tomcat8	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	Third Party
[SECURITY] [DLA 2077-1] tomcat7 security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Apache Tomcat: Multiple vulnerabilities (GLSA 202003-43) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
Debian -- Security Information -- DSA-4680-1 tomcat9	DEBIAN	<a href="https://www.debian.org">www.debian.org</a>	
USN-4251-1: Tomcat vulnerabilities   Ubuntu security notices   Ubuntu	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
Pony Mail!	CONFIRM	<a href="https://lists.apache.org">lists.apache.org</a>	Mailing Lis
Pony Mail!	MLIST	<a href="https://lists.apache.org">lists.apache.org</a>	
Oracle Critical Patch Update Advisory - April 2020	N/A	<a href="https://www.oracle.com">www.oracle.com</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
Pony Mail!		<a href="https://lists.apache.org">lists.apache.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[20283](#) Oracle Database 19c Critical OJVM Patch Update - April 2020

[20291](#) Oracle Database 18c Critical OJVM Patch Update - April 2020

[296077](#) Oracle Solaris 11.4 Support Repository Update (SRU) 18.4.0 Missing (CPUJAN2020)

[352283](#) Amazon Linux Security Update for tomcat7: AL2012-2020-297

[355093](#) Amazon Linux Security Advisory for tomcat : ALAS2-2023-2047

[356243](#) Amazon Linux Security Advisory for tomcat : ALASTOMCAT8.5-2023-013

<a href="#">356298</a> Amazon Linux Security Advisory for tomcat : ALASTOMCAT9-2023-008
<a href="#">730434</a> Update TITLE manually (JRASERVER-70487)
<a href="#">730441</a> Atlassian Jira Local Privilege Escalation Vulnerability (JRASERVER-70487)
<a href="#">730449</a> (JRASERVER-70487)
<a href="#">730995</a> Apache Tomcat Local Privilege Escalation Vulnerability (Unauthenticated Check)
<a href="#">981953</a> Java (maven) Security Update for org.apache.tomcat.embed:tomcat-embed-core (GHSA-hh3j-x4mc-g48r)

© [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](#)