



# CVE-2021-42340

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

## Summary

<b>CVE</b>	CVE-2021-42340
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-10-14 20:15:00 UTC
<b>Updated</b>	2023-11-07 03:39:00 UTC
<b>Description</b>	The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60

## Risk And Classification

**Problem Types:** CWE-772

## 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>	10.0.0	milestone10	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone1	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone2	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone3	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone4	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone5	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Hci</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Management Services For Element Software</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Management Services For Element Software And Netapp Hci</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Agile Engineering Data Management</a>	6.2.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Big Data Spatial And Graph</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Diameter Signaling Router</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hospitality Cruise Shipboard Property Management System</a>	20.1.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Managed File Transfer</a>	12.2.1.3.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Managed File Transfer</a>	12.2.1.4.0	All	All	All

Application	Oracle	Middleware Common Libraries And Tools	12.2.1.4.0	All	All	All
Application	Oracle	Payment Interface	19.1	All	All	All
Application	Oracle	Payment Interface	20.3	All	All	All
Application	Oracle	Retail Customer Insights	15.0.2	All	All	All
Application	Oracle	Retail Customer Insights	16.0.2	All	All	All
Application	Oracle	Retail Data Extractor For Merchandising	15.0.2	All	All	All
Application	Oracle	Retail Data Extractor For Merchandising	16.0.2	All	All	All
Application	Oracle	Retail Eftlink	21.0.0	All	All	All
Application	Oracle	Retail Financial Integration	16.0.1	All	All	All
Application	Oracle	Retail Financial Integration	19.0.0	All	All	All
Application	Oracle	Retail Store Inventory Management	14.0.4.13	All	All	All
Application	Oracle	Retail Store Inventory Management	14.1.3.14	All	All	All
Application	Oracle	Retail Store Inventory Management	14.1.3.5	All	All	All
Application	Oracle	Retail Store Inventory Management	15.0.3.3	All	All	All
Application	Oracle	Retail Store Inventory Management	15.0.3.8	All	All	All
Application	Oracle	Retail Store Inventory Management	16.0.3.7	All	All	All
Application	Oracle	Sd-wan Edge	9.0	All	All	All
Application	Oracle	Sd-wan Edge	9.1	All	All	All
Application	Oracle	Taleo Platform	All	All	All	All

## References

### Reference

[CVE-2021-42340 Apache Tomcat Vulnerability in NetApp Products | NetApp Product Security](#)

[Oracle Critical Patch Update Advisory - April 2022](#)

[\[myfaces-commits\] 2021 1021 \[myfaces-tobago\] branch tobago-5.x updated: build: workaround for CVE-2021-42340](#)

[Oracle Critical Patch Update Advisory - January 2022](#)

[Pony Mail!](#)

[Apache Tomcat: Multiple Vulnerabilities \(GLSA 202208-34\) — Gentoo security](#)

[Pony Mail!](#)

[Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities \(CVE-2022-0842, CVE-2022-0857, CVE-2022-0858,](#)

[Debian -- Security Information -- DSA-5009-1 tomcat9](#)

[Oracle Critical Patch Update Advisory - July 2022](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

150451 Apache Tomcat Denial of Service Vulnerability (CVE-2021-42340)
178896 Debian Security Update for tomcat9 (DSA 5009-1)
184230 Debian Security Update for tomcat9 (CVE-2021-42340)
20255 Oracle Database 19c Critical Patch Update - April 2022
20257 Oracle Database 21c Critical Patch Update - April 2022
20285 Oracle Database 19c Critical OJVM Patch Update - April 2022
239916 Red Hat Update for red hat jboss web server 5.6.0 (RHSA-2021:4861)
296066 Oracle Solaris 11.4 Support Repository Update (SRU) 40.107.3 Missing (CPUOCT2021)
352860 Amazon Linux Security Advisory for tomcat8: ALAS-2021-1546
356263 Amazon Linux Security Advisory for tomcat : ALASTOMCAT8.5-2023-006
356266 Amazon Linux Security Advisory for tomcat : ALASTOMCAT9-2023-006
710609 Gentoo Linux Apache Tomcat Multiple Vulnerabilities (GLSA 202208-34)
730242 Apache Tomcat Denial of Service (DoS) Vulnerability
730296 Atlassian Jira Server and Data Center Denial of Service (DoS) Vulnerability (JRASERVER-72914)
730327 Atlassian Jira Server Multiple Security Vulnerabilities (JRASERVER-73171, JRASERVER-73071, JRASERVER-73070)
730654 Apache Tomcat Denial of Service (DoS) Vulnerability (CVE-2021-42340)
730655 Apache Tomcat Denial of Service (DoS) Vulnerability (CVE-2021-42340)
730661 Apache Tomcat Denial of Service (DoS) Vulnerability (CVE-2021-42340)
730667 Apache Tomcat Denial of Service (DoS) Vulnerability (CVE-2021-42340)
980125 Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-wph7-x527-w3h5)

© [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](#)