



# CVE-2021-43980

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

## Summary

<b>CVE</b>	CVE-2021-43980
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-09-28 14:15:00 UTC
<b>Updated</b>	2022-11-10 04:00:00 UTC
<b>Description</b>	The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onw

## Risk And Classification

**Problem Types:** CWE-362

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	10.0.0	milestone1	All	All
Application	Apache	Tomcat	10.0.0	milestone10	All	All
Application	Apache	Tomcat	10.0.0	milestone2	All	All
Application	Apache	Tomcat	10.0.0	milestone3	All	All
Application	Apache	Tomcat	10.0.0	milestone4	All	All
Application	Apache	Tomcat	10.0.0	milestone5	All	All
Application	Apache	Tomcat	10.0.0	milestone6	All	All
Application	Apache	Tomcat	10.0.0	milestone7	All	All
Application	Apache	Tomcat	10.0.0	milestone8	All	All
Application	Apache	Tomcat	10.0.0	milestone9	All	All
Application	Apache	Tomcat	10.1.0	milestone1	All	All
Application	Apache	Tomcat	10.1.0	milestone10	All	All
Application	Apache	Tomcat	10.1.0	milestone11	All	All
Application	Apache	Tomcat	10.1.0	milestone12	All	All
Application	Apache	Tomcat	10.1.0	milestone2	All	All
Application	Apache	Tomcat	10.1.0	milestone3	All	All
Application	Apache	Tomcat	10.1.0	milestone4	All	All

Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone5	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone6	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone7	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone8	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	10.1.0	milestone9	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone1	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone2	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone3	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone4	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone5	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone6	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone7	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone8	All	All
Application	<a href="#">Apache</a>	<a href="#">Tomcat</a>	9.0.0	milestone9	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
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="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All

## References

Reference	Source	Link	Tags
oss-security - CVE-2021-43980: Apache Tomcat: Information disclosure	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
Debian -- Security Information -- DSA-5265-1 tomcat9	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
[SECURITY] [DLA 3160-1] tomcat9 security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	
<a href="https://lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3">lists.apache.org/thread/3jjqbsp6j88b198x5rmg99b1qr8ht3g3</a>	MISC	<a href="http://lists.apache.org">lists.apache.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** Thanks to Adam Thomas, Richard Hernandez and Ryan Schmitt for discovering the issue and working with the Tomcat security team to identify the root cause and appropriate fix.

## Legacy QID Mappings

150579 Apache Tomcat Information Disclosure Vulnerability (CVE-2021-43980)
181163 Debian Security Update for tomcat9 (DLA 3160-1)
181177 Debian Security Update for tomcat9 (DSA 5265-1)
183888 Debian Security Update for tomcat9 (CVE-2021-43980)
354897 Amazon Linux Security Advisory for tomcat8 : ALAS-2023-1732
355155 Amazon Linux Security Advisory for tomcat9 : ALAS2023-2023-176
356166 Amazon Linux Security Advisory for tomcat : ALASTOMCAT9-2023-005
356243 Amazon Linux Security Advisory for tomcat : ALASTOMCAT8.5-2023-013
730647 Apache Tomcat Information Disclosure Vulnerability (CVE-2021-43980)
730650 Apache Tomcat Information Disclosure Vulnerability (CVE-2021-43980)
730659 Apache Tomcat Information Disclosure Vulnerability (CVE-2021-43980)
730665 Apache Tomcat Information Disclosure Vulnerability (CVE-2021-43980)
752808 SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2022:4009-1)
752834 SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2022:4221-1)
752849 SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2022:4257-1)

© [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](#)**