



CVE-2022-34305

Published on: Not Yet Published

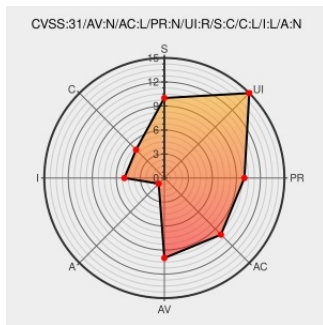
Last Modified on: 07/29/2022 08:15:00 PM UTC

CVE-2022-34305

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Tomcat** from **Apache** contain the following vulnerability:

In Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.5.81 the Form authentication example in the examples web application displayed user provided data without filtering, exposing a XSS vulnerability.

CVE-2022-34305 has been assigned by security@apache.org to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Apache Software Foundation - Apache Tomcat** version = **8.5.50 to 8.5.81**

Affected Vendor/Software: **Apache Software Foundation - Apache Tomcat** version = **9.0.30 to 9.0.64**

Affected Vendor/Software: **Apache Software Foundation - Apache Tomcat** version = **10.0.0-M1 to 10.0.22**

Affected Vendor/Software: **Apache Software Foundation - Apache Tomcat** version = **10.1.0-M1 to 10.1.0-M16**




CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - CVE-2022-34305: Apache Tomcat: XSS in examples web application	www.openwall.com text/html	 MLIST [oss-security] 20220623 CVE-2022-34305: Apache Tomcat: XSS in examples web application
CVE-2022-34305 Apache Tomcat Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20220729-0006/
No Description Provided	lists.apache.org text/html	 CONFIRM N/A

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers





- [150541](#) Apache Tomcat Cross-Site Scripting(XSS) Vulnerability (CVE-2022-34305)
- [690921](#) Free Berkeley Software Distribution (FreeBSD) Security Update for tomcat (e2e7faf9-1b51-11ed-ae46-002b67dfc673)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	milestone13	All	All
Application	Apache	Tomcat	10.1.0	milestone14	All	All
Application	Apache	Tomcat	10.1.0	milestone15	All	All
Application	Apache	Tomcat	10.1.0	milestone16	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	Apache	Tomcat	10.1.0	milestone5	All	All
Application	Apache	Tomcat	10.1.0	milestone6	All	All
Application	Apache	Tomcat	10.1.0	milestone7	All	All
Application	Apache	Tomcat	10.1.0	milestone8	All	All
Application	Apache	Tomcat	10.1.0	milestone9	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	All	All	All	All

cpe:2.3:a:apache:tomcat:10.1.0:milestone1:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone10:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone11:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone12:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone13:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone14:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone15:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone16:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone2:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone3:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone4:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone5:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone6:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone7:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone8:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:10.1.0:milestone9:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:*:*:*:*:*:
cpe:2.3:a:apache:tomcat:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVereport	CVE-2022-34305 : In #Apache Tomcat 10.1.0-M1 to 10.1.0-M16, 10.0.0-M1 to 10.0.22, 9.0.30 to 9.0.64 and 8.5.50 to 8.... twitter.com/i/web/status/1...	2022-06-23 10:36:36
 @Inceptus3	New Vulnerability: CVE-2022-34305 #InceptusSecure #UnderOurProtection	2022-06-23 12:15:01
 @LinInfoSec	Tomcat - CVE-2022-34305: lists.apache.org/thread/k04zk0n...	2022-06-23 13:02:06
 /r/netcve	CVE-2022-34305	2022-06-23 11:38:55

© CVE.report 2022   |

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](#)