



# CVE-2021-33037

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

## Summary

<b>CVE</b>	CVE-2021-33037
<b>State</b>	PUBLIC
<b>Assigner</b>	security@apache.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-12 15:15:00 UTC
<b>Updated</b>	2023-11-07 03:35:00 UTC
<b>Description</b>	Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encod

## Risk And Classification

**Problem Types:** CWE-444

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Lang
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="#">Tomee</a>	8.0.6	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>	9.0	All	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	All	All	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	-	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_1	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_10	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_2	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_3	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_4	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_5	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_6	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_7	All	All
Application	<a href="#">Mcafee</a>	<a href="#">Epolicy Orchestrator</a>	5.10.0	update_8	All	All

Application	Mcafee	Epolicy Orchestrator	5.10.0	update_9	All	All
Application	Oracle	Agile Plm	9.3.6	All	All	All
Application	Oracle	Communications Cloud Native Core Policy	1.14.0	All	All	All
Application	Oracle	Communications Cloud Native Core Service Communication Proxy	1.14.0	All	All	All
Application	Oracle	Communications Diameter Signaling Router	All	All	All	All
Application	Oracle	Communications Diameter Signaling Router	All	All	All	All
Application	Oracle	Communications Instant Messaging Server	10.0.1.5.0	All	All	All
Application	Oracle	Communications Policy Management	12.5.0	All	All	All
Application	Oracle	Communications Pricing Design Center	12.0.0.3.0	All	All	All
Application	Oracle	Communications Session Report Manager	All	All	All	All
Application	Oracle	Communications Session Route Manager	All	All	All	All
Application	Oracle	Graph Server And Client	All	All	All	All
Application	Oracle	Healthcare Translational Research	4.1.0	All	All	All
Application	Oracle	Hospitality Cruise Shipboard Property Management System	20.1.0	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.1	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.2	All	All	All
Application	Oracle	Instantis Enterprisetrack	17.3	All	All	All
Application	Oracle	Managed File Transfer	12.2.1.3.0	All	All	All
Application	Oracle	Managed File Transfer	12.2.1.4.0	All	All	All
Application	Oracle	Mysql Enterprise Monitor	All	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	Secure Global Desktop	5.6	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.1.1	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.2.2	All	All	All
Application	Oracle	Utilities Testing Accelerator	6.0.0.3.1	All	All	All

## References

### Reference

Pony Mail!

[tomee-commits] 20210913 [jira] [Commented] (TOME-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037

[tomee-commits] 20210914 [jira] [Commented] (TOME-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037

July 2021 Apache Tomcat Vulnerabilities in NetApp Products | NetApp Product Security

Oracle Critical Patch Update Advisory - April 2022

Security Bulletin - ePolicy Orchestrator update addresses two product vulnerabilities (CVE-2021-31834 and CVE-2021-31835) and updates Ja

Pony Mail!

Oracle Critical Patch Update Advisory - July 2021

[tomee-commits] 20210916 [jira] [Resolved] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037

[tomee-commits] 20210728 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037

Pony Mail!

Oracle Critical Patch Update Advisory - October 2021

[SECURITY] [DLA 2733-1] tomcat8 security update

Pony Mail!

Oracle Critical Patch Update Advisory - January 2022

Pony Mail!

Debian -- Security Information -- DSA-4952-1 tomcat9

Pony Mail!

Apache Tomcat: Multiple Vulnerabilities (GLSA 202208-34) — Gentoo security

[tomee-commits] 20210728 [jira] [Created] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037

Pony Mail!

[tomee-commits] 20210830 [jira] [Commented] (TOMEE-3778) Update embedded Tomcat to 9.0.48 or later to address CVE-2021-33037

CVE Program record

NVD vulnerability detail



## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** The Apache Tomcat Security Team would like to thank Bahruz Jabiyev, Steven Sprecher and Kaan Onarlioglu of NEU seclab for identifying and reporting this issue.

## Legacy QID Mappings

[150367](#) Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2021-33037)

[178743](#) Debian Security Update for tomcat8 (DLA 2733-1)

[178746](#) Debian Security Update for tomcat9 (DSA 4952-1)

[180184](#) Debian Security Update for tomcat9 (CVE-2021-33037)

[198724](#) Ubuntu Security Notification for Tomcat Vulnerabilities (USN-5360-1)

[239916](#) Red Hat Update for red hat jboss web server 5.6.0 (RHSA-2021:4861)

[296065](#) Oracle Solaris 11.4 Support Repository Update (SRU) 39.107.1 Missing (CPUOCT2021)

[352800](#) Amazon Linux Security Advisory for tomcat8: ALAS-2021-1535

<a href="#">356206</a> Amazon Linux Security Advisory for tomcat : ALASTOMCAT9-2023-007
<a href="#">356267</a> Amazon Linux Security Advisory for tomcat : ALASTOMCAT8.5-2023-007
<a href="#">376076</a> F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Apache Tomcat Vulnerability (K32469285)
<a href="#">690073</a> Free Berkeley Software Distribution (FreeBSD) Security Update for tomcat (d34bef0b-f312-11eb-b12b-fc4dd43e2b6a)
<a href="#">710609</a> Gentoo Linux Apache Tomcat Multiple Vulnerabilities (GLSA 202208-34)
<a href="#">730141</a> Apache Tomcat HTTP Request Smuggling Vulnerability (CVE-2021-33037)
<a href="#">730327</a> Atlassian Jira Server Multiple Security Vulnerabilities (JRASERVER-73171, JRASERVER-73071, JRASERVER-73070)
<a href="#">751320</a> SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2021:3602-1)
<a href="#">751355</a> OpenSUSE Security Update for tomcat (openSUSE-SU-2021:3672-1)
<a href="#">751364</a> SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2021:3669-1)
<a href="#">751365</a> SUSE Enterprise Linux Security Update for tomcat (SUSE-SU-2021:3670-1)
<a href="#">751370</a> OpenSUSE Security Update for tomcat (openSUSE-SU-2021:1490-1)
<a href="#">980269</a> Java (maven) Security Update for org.apache.tomcat:tomcat (GHSA-4vww-mc66-62m6)

© [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](#)**