

CVE-2016-8735

Apache Tomcat Remote Code Execution Vulnerability

Exigent

CISA KEV since May 12, 2023

Actively exploited

Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types.

EVRS

85/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.903

99.8th percentile · FIRST

CISA DEADLINE

Jun 2, 2023

KEV since 2023 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.903 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · GHSA-cw54-59pw-4g8c lists 2 more affected packages · 11 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.tomcat:tomcat-catalina	< 6.0.48	6.0.48	GitHub
org.apache.tomcat:tomcat-catalina	≥ 7.0.0, < 7.0.73	7.0.73	GitHub
org.apache.tomcat:tomcat-catalina	≥ 8.0.0, < 8.0.39	8.0.39	GitHub
org.apache.tomcat:tomcat-catalina	≥ 8.5.0, < 8.5.7	8.5.7	GitHub
org.apache.tomcat:tomcat-catalina	≥ 9.0.0.M1, < 9.0.0.M12	9.0.0.M12	GitHub
org.apache.tomcat:tomcat-catalina-jmx-remote	< 6.0.48	6.0.48	GitHub
org.apache.tomcat:tomcat-catalina-jmx-remote	≥ 7.0.0, < 7.0.73	7.0.73	GitHub
org.apache.tomcat:tomcat-catalina-jmx-remote	≥ 8.0.0, < 8.0.39	8.0.39	GitHub

PACKAGE	AFFECTED	FIXED IN	SOURCE
tomcat	$< 6.0.48$ $\geq 7.0.0 < 7.0.73$ $\geq 8.0 < 8.0.39$ $\geq 8.5.0 < 8.5.7$ $9.0.0$	no fixed version listed	NVD
7-mode transition tool	—	no fixed version listed	NVD
oncommand insight	—	no fixed version listed	NVD
oncommand shift	—	no fixed version listed	NVD
snap creator framework	—	no fixed version listed	NVD
jboss enterprise web server	3.0.0	no fixed version listed	NVD
agile engineering data management	6.1.3 6.2.0 6.2.1.0	no fixed version listed	NVD
agile product lifecycle management	9.3.5 9.3.6	no fixed version listed	NVD

Sources

Vendor guidance	lists.apache.org/thread.html/343558d982879bf88ec20dbf707f8c11255f8e219e81d45c4f8d0551%40%3Cdev.tomcat.apache.org%3E	Additional guidance	access.redhat.com/errata/RHSA-2017:0455
tomcat.apache.org	tomcat.apache.org/security-9.html	NVD	nvd.nist.gov/vuln/detail/CVE-2016-8735
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	GitHub advisory	github.com/advisories/GHSA-cw54-59pw-4g8c
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-3642	Current data	evulnable.com/vulnerability-management/cve/CVE-2016-8735

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.