

CVE-2017-12615

Apache Tomcat on Windows Remote Code Execution Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Ransomware use known

When running Apache Tomcat 7.0.0 to 7.0.79 on Windows with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.

EVRS 91 /100 Immediate priority	CVSS V3.1 8.1 High · NVD	EPSS 0.996 99.95th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.996 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions · 15 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
org.apache.tomcat.embed:tomcat-embed-core	≥ 7.0.0, < 7.0.79	7.0.79	GitHub
tomcat	≥ 7.0.0 ≤ 7.0.79	after 7.0.79	NVD
7-mode transition tool	—	no fixed version listed	NVD
oncommand balance	—	no fixed version listed	NVD
oncommand shift	—	no fixed version listed	NVD
enterprise linux server update services for sap solutions	7.4 7.6 7.7	no fixed version listed	NVD
jboss enterprise web server	2.0.0 3.0.0	no fixed version listed	NVD
jboss enterprise web server text-only advisories	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD



Sources

Vendor guidance	lists.apache.org/thread.html/388a323769f1dffa84c9ec905455aa73fbc20338e3c7eb131457f708%40%3Cdev.tomcat.apache.org%3Envd.nist.gov/vuln/detail/CVE-2017-12615	Additional guidance	access.redhat.com/errata/RHSA-2017:3113
NVD	nvd.nist.gov/vuln/detail/CVE-2017-12615	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-pjfr-qf3p-3q25	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2018-0654
Current data	evulnable.com/vulnerability-management/cve/CVE-2017-12615		

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