CVE-2017-12617

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-12617
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-04 01:29:02 UTC
Updated	2026-04-21 17:03:52 UTC
Description	When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTT

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.943560000 probability, percentile 0.999610000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-25; due 2022-04-15; ransomware use Unknown

Problem Types: CWE-434 | Remote Code Execution | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

CISA Known Exploited Vulnerability

Vendor	Apache
Product	Tomcat
Name	Apache Tomcat Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2017-12617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Tomcat	affected 9.0.0.M1 to 9.0.0	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 8.5.0 to 8.5.22	Not specified

CNA	Apache Software Foundation	Apache Tomcat	affected 8.0.0.RC1 to 8.0.46	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 7.0.0 to 7.0.81	Not specified

References

Reference
Apache Tomcat HTTP PUT Request Processing Flaw Lets Remote Users Execute Arbitrary JSP Code on the Target System - SecurityTracke
Red Hat Customer Portal
support.f5.com/csp/article/K53173544
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Red Hat Customer Portal
Document Display | HPE Support Center
www.cisa.gov/known-exploited-vulnerabilities-catalog
Red Hat Customer Portal
Apache Tomcat CVE-2017-12617 Incomplete Fix Remote Code Execution Vulnerability
Red Hat Customer Portal
Pony Mail!
January 2018 MySQL vulnerabilities in NetApp Products | NetApp Product Security
Tomcat - Remote Code Execution via JSP Upload Bypass (Metasploit)
CVE-2017-12617 Apache Tomcat Vulnerability in NetApp Products | NetApp Product Security
Red Hat Customer Portal
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update - January 2018
Pony Mail!
Red Hat Customer Portal
Oracle Critical Patch Update - April 2018
Red Hat Customer Portal
Pony Mail!
Pony Mail!

Document Display | HPE Support Center
Red Hat Customer Portal
Red Hat Customer Portal
Pony Mail!
Oracle Critical Patch Update Advisory - April 2019
CPU July 2018
USN-3665-1: Tomcat vulnerabilities | Ubuntu security notices
Pony Mail!
Red Hat Customer Portal
Pony Mail!
Pony Mail!
Pony Mail!
[SECURITY] [DLA 1166-1] tomcat7 security update
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
Pony Mail!
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-03-25T00:00:00.000Z	CVE-2017-12617 added to CISA KEV

Legacy QID Mappings

20294 Oracle Database 12.2.0.1 Critical OJVM Patch Update - January 2018

378318 Virtuozzo Linux Security Update for tomcat6-lib (VZLSA-2017:3080)