



# CVE-2016-8747

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

## Summary

<b>CVE</b>	CVE-2016-8747
<b>State</b>	PUBLISHED
<b>Assigner</b>	apache
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-14 09:59:00 UTC
<b>Updated</b>	2026-04-16 21:06:47 UTC
<b>Description</b>	An information disclosure issue was discovered in Apache Tomcat 8.5.7 to 8.5.9 and 9.0.0.M11 to 9.0.0.M15 in reverse-pro

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from nvd@nist.gov

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

**EPSS:** 0.031490000 probability, percentile 0.869110000 (date 2026-04-16)

**Problem Types:** CWE-200 | Information disclosure | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	5		AV:N/AC:L/Au:N/C:P/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

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

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Tomcat	All	All	All	All
Application	Apache	Tomcat	9.0.0	milestone11	All	All
Application	Apache	Tomcat	9.0.0	milestone12	All	All
Application	Apache	Tomcat	9.0.0	milestone13	All	All
Application	Apache	Tomcat	9.0.0	milestone14	All	All
Application	Apache	Tomcat	9.0.0	milestone15	All	All
Application	Netapp	Oncommand Insight	-	All	All	All
Application	Netapp	Oncommand Shift	-	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Tomcat	affected 8.5.7 to 8.5.9	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 9.0.0.M11 to 9.0.0.M15	Not specified

### References

Reference	Source	L
Pony Mail!	af854a3a-2127-422b-91ae-364da2661108	li
Pony Mail!	af854a3a-2127-422b-91ae-364da2661108	li
CVE-2016-8747 Apache Tomcat Vulnerability in NetApp Products   NetApp Product Security	af854a3a-2127-422b-91ae-364da2661108	s
Apache Tomcat® - Apache Tomcat 8 vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	tc
Pony Mail!	af854a3a-2127-422b-91ae-364da2661108	li
Apache Tomcat CVE-2016-8747 Information Disclosure Vulnerability	af854a3a-2127-422b-91ae-364da2661108	w
Pony Mail!	af854a3a-2127-422b-91ae-364da2661108	li
[Apache-SVN] Revision 1774161	af854a3a-2127-422b-91ae-364da2661108	s
[Apache-SVN] Revision 1774166	af854a3a-2127-422b-91ae-364da2661108	s
Apache Tomcat - Apache Tomcat 8 vulnerabilities	af854a3a-2127-422b-91ae-364da2661108	tc
Pony Mail!	af854a3a-2127-422b-91ae-364da2661108	li
Pony Mail!	af854a3a-2127-422b-91ae-364da2661108	li
Pony Mail!	MITRE	li
Pony Mail!	MITRE	li
Pony Mail!	MITRE	li
Pony Mail!	MITRE	li
Pony Mail!	MITRE	li
Pony Mail!	MITRE	li
Pony Mail!	MITRE	li
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[996792](#) Java (Maven) Security Update for org.apache.tomcat:tomcat (GHSA-fjwp-r6fm-q6qw)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)