Apache Tomcat: OCSP checks sometimes soft-fail with FFM even when soft-fail is disabled

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

Summary

CVE	CVE-2026-34500
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 20:16:25 UTC
Updated	2026-04-10 15:16:24 UTC
Description	CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled and FFM is used in A

Risk And Classification

Primary CVSS: v3.1 6.5 MEDIUM from ADP

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

EPSS: 0.000360000 probability, percentile 0.107180000 (date 2026-04-10)

Problem Types: CWE-287 | CLIENT_CERT authentication does not fail as expected for some scenarios when soft fail is disabled | CWE-287 CWE-287 Improper Authentication

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Tomcat	affected 11.0.0-M14 11.0.20 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 10.1.22 10.1.53 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 9.0.92 9.0.116 semver	Not specified

References

Reference	Source	Link	Tags
lists.apache.org/thread/7rcl4zdxryc8hy3htyfyxkbqpxjtfdl2	security@apache.org	lists.apache.org	
www.openwall.com/lists/oss-security/2026/04/09/29	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

Vendor Comments And Credit

Discovery Credit

CNA: Haruki Oyama (Waseda University) (en)

There are currently no legacy QID mappings associated with this CVE.