Apache Tomcat: Occasionally open redirect

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

Summary

CVE	CVE-2026-25854
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 20:16:24 UTC
Updated	2026-04-10 19:16:21 UTC
Description	Occasional URL redirection to untrusted Site ('Open Redirect') vulnerability in Apache Tomcat via the LoadBalancerDrainin

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from ADP

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

EPSS: 0.000050000 probability, percentile 0.002770000 (date 2026-04-10)

Problem Types: CWE-601 | CWE-601 CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Tomcat	affected 11.0.0-M1 11.0.18 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 10.1.0-M1 10.1.52 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 9.0.0.M23 9.0.115 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 8.5.30 8.5.100 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	unaffected 7.0.109 semver	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/04/09/21	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	
lists.apache.org/thread/ghct3b6o74bp2vm7q875s1zh0dqrz3h0	security@apache.org	lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

Vendor Comments And Credit

Discovery Credit

CNA: gregk4sec (https://github.com/gregk4sec) (en)

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