



Apache Tomcat: EncryptInterceptor vulnerable to padding oracle attack by default

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

Summary

CVE	CVE-2026-29146
State	PUBLISHED
Assigner	apache
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 20:16:24 UTC
Updated	2026-04-14 12:56:21 UTC
Description	Padding Oracle vulnerability in Apache Tomcat's EncryptInterceptor with default configuration. This issue affects Apache Tomcat versions 9.0.0 through 9.0.90, 10.0.0 through 10.0.10, and 11.0.0 through 11.0.10. The vulnerability is caused by a padding oracle attack on the EncryptInterceptor class, which is used to encrypt sensitive information in the response. The attack is possible because the EncryptInterceptor class does not properly validate the padding in the ciphertext, allowing an attacker to determine the padding value by observing the error messages returned by the server.

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

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

EPSS: 0.001040000 probability, percentile 0.284770000 (date 2026-04-15)

Problem Types: CWE-209 | CWE-642 | Padding Oracle | CWE-209 CWE-209 Generation of Error Message Containing Sensitive Information | CWE-642 CWE-642 External Control of Critical State Data

Version	Source	Type	Score	Severity	Vector
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

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

NVD Known Affected Configurations (CPE 2.3)

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

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 10.0.0-M1 10.1.52 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 9.0.13 9.0.115 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 8.5.38 8.5.100 semver	Not specified
CNA	Apache Software Foundation	Apache Tomcat	affected 7.0.100 7.0.109 semver	Not specified

References

Reference	Source	Link	Tags
www.openwall.com/lists/oss-security/2026/04/09/24	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing Lis
lists.apache.org/thread/lzt04z2pb3dc5tk85obn80xygw3z1p0w	security@apache.org	lists.apache.org	Mailing Lis
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

Vendor Comments And Credit

Discovery Credit

CNA: Uri Katz and Avi Lumelsky (Oligo Security) (en)

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

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