



# Apache Camel JMS, Apache Camel CoAP, Apache Camel Google PubSub: Incomplete fix for CVE-2025-27636 in non-HTTP HeaderFilterStrategies (camel-jms, camel-sjms, camel-coap, camel-google-pubsub) allows case-variant header injection

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

## Summary

<b>CVE</b>	CVE-2026-40453
<b>State</b>	PUBLISHED
<b>Assigner</b>	apache
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-27 09:16:01 UTC
<b>Updated</b>	2026-04-28 19:43:55 UTC
<b>Description</b>	The fix for CVE-2025-27636 added setLowerCase(true) to HttpHeadersStrategy so that case-variant header names suc

## Risk And Classification

**Primary CVSS:** v3.1 9.9 CRITICAL from ADP

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

**EPSS:** 0.000580000 probability, percentile 0.179010000 (date 2026-04-27)

**Problem Types:** CWE-178 | CWE-178 CWE-178 Improper Handling of Case Sensitivity

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.9	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

None

Scope

Changed

Confidentiality

High

Integrity

High

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Apache Software Foundation	Apache Camel JMS	affected 3.0.0 4.14.6 semver	Not specified
CNA	Apache Software Foundation	Apache Camel JMS	affected 4.15.0 4.18.2 semver	Not specified
CNA	Apache Software Foundation	Apache Camel JMS	affected 4.19.0 4.20.0 semver	Not specified
CNA	Apache Software Foundation	Apache Camel CoAP	affected 3.0.0 4.14.6 semver	Not specified
CNA	Apache Software Foundation	Apache Camel CoAP	affected 4.15.0 4.18.2 semver	Not specified
CNA	Apache Software Foundation	Apache Camel CoAP	affected 4.19.0 4.20.0 semver	Not specified
CNA	Apache Software Foundation	Apache Camel Google PubSub	affected 3.0.0 4.14.6 semver	Not specified
CNA	Apache Software Foundation	Apache Camel Google PubSub	affected 4.15.0 4.18.2 semver	Not specified
CNA	Apache Software Foundation	Apache Camel Google PubSub	affected 4.19.0 4.20.0 semver	Not specified

### References

Reference	Source	Link	Tags
camel.apache.org/security/CVE-2026-40453.html	security@apache.org	camel.apache.org	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Saroj Khadka (en)

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

© [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](#)