



# Apache Camel: Unsafe Deserialization of JMS ObjectMessage in camel-jms, camel-sjms, camel-sjms2 and camel-amqp

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

## Summary

<b>CVE</b>	CVE-2026-40860
<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 19:42:46 UTC
<b>Description</b>	JmsBinding.extractBodyFromJms() in camel-jms, and the equivalent JmsBinding class in camel-sjms, deserialized the payload

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from ADP

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

**EPSS:** 0.003020000 probability, percentile 0.534930000 (date 2026-04-27)

**Problem Types:** CWE-502 | CWE-502 CWE-502 Deserialization of Untrusted Data

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/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	affected 3.0.0 4.14.7 semver	Not specified
CNA	Apache Software Foundation	Apache Camel	affected 4.15.0 4.18.2 semver	Not specified
CNA	Apache Software Foundation	Apache Camel	affected 4.19.0 4.20.0 semver	Not specified

### References

Reference	Source	Link	Tags
camel.apache.org/security/CVE-2026-40860.html	security@apache.org	camel.apache.org	Vendor Advisory
www.openwall.com/lists/oss-security/2026/04/26/10	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com	Mailing List, Third Party
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:** Venkatraman Kumar from Securin (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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)