



# CVE-2015-5348

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

| Summary         |                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2015-5348                                                                                                              |
| State           | PUBLISHED                                                                                                                  |
| Assigner        | redhat                                                                                                                     |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                               |
| Published       | 2016-04-15 15:59:00 UTC                                                                                                    |
| Updated         | 2026-05-06 22:30:45 UTC                                                                                                    |
| Description     | Apache Camel 2.6.x through 2.14.x, 2.15.x before 2.15.5, and 2.16.x before 2.16.1, when using (1) camel-jetty or (2) camel |

Risk And Classification

Primary CVSS: v3.0 8.1 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-19 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 8.1   | HIGH     | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H |
| 2.0     | nvd@nist.gov | Primary | 6.8   |          | AV:N/AC:M/Au:N/C:P/I:P/A:P                   |

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

| NVD Known Affected Configurations (CPE 2.3) |        |         |         |        |         |          |
|---------------------------------------------|--------|---------|---------|--------|---------|----------|
| Type                                        | Vendor | Product | Version | Update | Edition | Language |
| Application                                 | Apache | Camel   | 2.10.0  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.1  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.2  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.3  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.4  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.5  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.6  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.10.7  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.11.0  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.11.1  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.11.2  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.11.3  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.11.4  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.12.0  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.12.1  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.12.2  | All    | All     | All      |
| Application                                 | Apache | Camel   | 2.12.3  | All    | All     | All      |

|             |                        |                       |        |     |     |     |
|-------------|------------------------|-----------------------|--------|-----|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.12.4 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.12.5 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.13.0 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.13.1 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.13.2 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.13.3 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.13.4 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.14.0 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.14.1 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.14.2 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.14.3 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.14.4 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.15.0 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.15.1 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.15.2 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.15.3 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.15.4 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.16.0 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.6.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.7.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.7.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.7.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.7.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.7.4  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.7.5  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.3  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.4  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.5  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.8.6  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.0  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.1  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.2  | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.3  | All | All | All |

|             |                        |                       |       |     |     |     |
|-------------|------------------------|-----------------------|-------|-----|-----|-----|
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.3 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.4 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.5 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.6 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.7 | All | All | All |
| Application | <a href="#">Apache</a> | <a href="#">Camel</a> | 2.9.8 | All | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |  |
|-----------------------------------|--------------------|---------------------|--------------|---------------|--|
| Source                            | Vendor             | Product             | Version      | Platforms     |  |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |  |

| References                                                                                   |                                      |                     |  |
|----------------------------------------------------------------------------------------------|--------------------------------------|---------------------|--|
| Reference                                                                                    | Source                               | Link                |  |
| Apache Camel CVE-2015-5348 Information Disclosure Vulnerability                              | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">w</a>   |  |
| Apache Camel Java Object Deserialization ≈ Packet Storm                                      | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">pe</a>  |  |
| SecurityFocus                                                                                | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">w</a>   |  |
| Red Hat Customer Portal                                                                      | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">rh</a>  |  |
| camel.apache.org/security-advisories.data/CVE-2015-5348.txt.asc                              | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">ce</a>  |  |
| [CAMEL-9309] camel-jetty - Make it easier to turn on off java transport over http - ASF JIRA | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">is</a>  |  |
| Pony Mail!                                                                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">lis</a> |  |
| Pony Mail!                                                                                   | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">lis</a> |  |
| Pony Mail!                                                                                   | MITRE                                | <a href="#">lis</a> |  |
| Pony Mail!                                                                                   | MITRE                                | <a href="#">lis</a> |  |
| CVE Program record                                                                           | CVE.ORG                              | <a href="#">w</a>   |  |
| NVD vulnerability detail                                                                     | NVD                                  | <a href="#">nv</a>  |  |

No vendor comments have been submitted for this CVE.

| Legacy QID Mappings                                                                                          |
|--------------------------------------------------------------------------------------------------------------|
| <a href="#">981440</a> Java (maven) Security Update for org.apache.camel:camel-servlet (GHSA-26v6-w6fw-rh94) |

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)