



# Static resource cache poisoning in Spring MVC and WebFlux

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

## Summary

<b>CVE</b>	CVE-2026-22741
<b>State</b>	PUBLISHED
<b>Assigner</b>	vmware
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-29 12:16:18 UTC
<b>Updated</b>	2026-05-04 14:51:05 UTC
<b>Description</b>	Spring MVC and WebFlux applications are vulnerable to cache poisoning when resolving static resources. More precisely, a

## Risk And Classification

**Primary CVSS:** v3.1 3.1 LOW from security@vmware.com

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

**EPSS:** 0.000470000 probability, percentile 0.142400000 (date 2026-05-03)

**Problem Types:** CWE-524 | CWE-524 CWE-524 Information Exposure Through Caching

Version	Source	Type	Score	Severity	Vector
3.1	security@vmware.com	Secondary	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L
3.1	CNA	CVSS	3.1	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

Low

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	VMware	Spring Framework	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	VMware	Spring Framework	affected 7.0.0 7.0.7 oss	Not specified
CNA	VMware	Spring Framework	affected 6.2.0 6.2.18 oss	Not specified
CNA	VMware	Spring Framework	affected 6.1.0 6.1.27 commercial	Not specified
CNA	VMware	Spring Framework	affected 5.3.0 5.3.48 commercial	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator">nvd.nist.gov/vuln-metrics/cvss/v3-calculator</a>	security@vmware.com	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	US Government Resource
<a href="https://spring.io/security/cve-2026-22741">spring.io/security/cve-2026-22741</a>	security@vmware.com	<a href="https://spring.io">spring.io</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** Yuki Matsuhashi . (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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org). This site includes MITRE data granted under the following [license](https://www.mitre.org).

Free CVE JSON API [cve.report/api](https://cve.report/api)

