

Spring Security Advisories



CVE-2026-22741: Static resource cache poisoning in Spring MVC and WebFlux

LOW | APRIL 17, 2026 | CVE-2026-22741

Description

Spring MVC and WebFlux applications are vulnerable to cache poisoning when resolving static resources.

More precisely, an application can be vulnerable when all the following are true:

- the application is using Spring MVC or Spring WebFlux
- the application is configuring the [resource chain support](#) with caching enabled
- the application adds support for encoded resources resolution
- the resource cache must be empty when the attacker has access to the application

When all the conditions above are met, the attacker can send malicious requests and poison the resource cache with resources using the wrong encoding. This can cause a denial of service by breaking the front-end application for clients.

Affected Spring Products and Versions

Spring Framework:

Reporting a vulnerability

To report a security vulnerability for a project within the Spring portfolio, see the [Security Policy](#)

- 6.1.0 - 6.1.26
- 5.3.0 - 5.3.47

Older, unsupported versions are also vulnerable.

Mitigation

Users of affected versions should upgrade to the corresponding fixed version.

Affected version(s)	Fix version	Availability
7.0.x	7.0.7	OSS
6.2.x	6.2.18	OSS
6.1.x	6.1.27	Commercial
5.3.x	5.3.48	Commercial

No further mitigation steps are necessary.

Credit

This issue was responsibly reported by [Yuki Matsuhashi](#).

References

- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L&version=3.1>

History

- 2026-04-17: Initial vulnerability report published.

Get ahead

VMware offers training and certification to turbocharge your progress.

[Learn more](#)

Get support

Tanzu Spring offers support and binaries for OpenJDK™, Spring, and Apache Tomcat® in one simple subscription.

[Learn more](#)

Upcoming events

Check out all the upcoming events in the Spring community.

[View all](#)

Why Spring

- Generative AI
- Microservices
- Reactive
- Event Driven
- Cloud
- Web Applications
- Serverless
- Batch

Learn

- Quickstart
- Guides
- Courses
- Get Certified

Projects

Resources

- Blog
- Release Calendar
- Version Mappings
- Release Highlights
- Security Advisories

Community

- Events
- Authors

Enterprise

- Long-term Support
- Automated Upgrades
- Governance and Compliance
- Modern App Development

Thank You

Get the Spring newsletter

Stay connected with the Spring newsletter



Copyright © 2005 - 2026 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

[Terms of Use](#) • [Privacy](#) • [Trademark Guidelines](#)

Apache[®], Apache Tomcat[®], Apache Kafka[®], Apache Cassandra[™], and Apache Geode[™] are trademarks or registered trademarks of the Apache Software Foundation in the United States and/or other countries. Java[™], Java[™] SE, Java[™] EE, and OpenJDK[™] are trademarks of Oracle and/or its affiliates. Kubernetes[®] is a registered trademark of the Linux Foundation in the United States and other countries. Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries. Windows[®] and Microsoft[®] Azure are registered trademarks of Microsoft Corporation. "AWS" and "Amazon Web Services" are trademarks or registered trademarks of Amazon.com Inc. or its affiliates. All other trademarks and copyrights are property of their respective owners and are only mentioned for informative purposes. Other names may be trademarks of their respective owners.