

## Spring Security Advisories

[RSS feed](#)

# CVE-2026-22753: Servlet Path Not Correctly Included in Path Matching of HttpSecurity#securityMatchers

**HIGH | APRIL 20, 2026 | CVE-2026-22753**

## Description

If an application is using `securityMatchers(String)` and a `PathPatternRequestMatcher.Builder` bean to prepend a servlet path, matching requests to that filter chain may fail and its related security components will not be exercised as intended by the application. This can lead to the authentication, authorization, and other security controls being rendered inactive on intended requests.

If you are not using `securityMatchers(String)`, you are not affected. Also, if you are not configuring a servlet path or are not using a `PathPatternRequestMatcher.Builder` bean to describe the servlet path, you are not affected.

If you are using Spring Boot, it may not be readily apparent to you if you are using a `PathPatternRequestMatcher.Builder` bean to prepend a servlet path. One common way to determine this is by looking for the Spring Boot property `spring.mvc.servlet.path` in your application; it may have a value like `/api` or `/mvc`.

## Affected Spring Products and Versions

Spring Security:

- 7.0.0 - 7.0.4

Spring Security 6.x and earlier are not affected; the described interaction involves Spring Security 7's integration between string-based matchers and a published `PathPatternRequestMatcher.Builder` bean.

## Mitigation

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

Affected version(s)	Fix version	Availability
7.0.x	7.0.5	OSS

If you are not able to upgrade, you can place the servlet path directly in the matcher pattern as follows:

```
http
    .securityMatchers("/servlet-path/admin/**")
    // ...
```

## Reporting a vulnerability

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

The issue was identified and responsibly reported by [npep](#) & [carinas](#) / [npepsec](#) agent.

## References

- <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:U/RL:O/RC:C/CR:L/IR:H/AR:L/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:N/MI:H/MA:N&version=3.1>

## History

- 2026-04-20: Initial vulnerability report published.

### Get ahead

VMware offers training and certification to turbo-charge 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

**SUBSCRIBE**

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.