

Spring Security Advisories

[RSS feed](#)

CVE-2026-22754: Servlet Path Not Correctly Included in Path Matching of XML Authorization Rules

Reporting a vulnerability

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

HIGH | APRIL 20, 2026 | CVE-2026-22754

Description

If an application uses

`<sec:intercept-url servlet-path="/servlet-path" pattern="/endpoint/**"/>` to define the servlet path for computing a path matcher, then the servlet path is not included and the related authorization rules are not exercised. This can lead to an authorization bypass.

Affected Spring Products and Versions

Spring Security:

- 7.0.0 - 7.0.4

Spring Security 6.x and earlier are not affected; the described issue applies to XML

`intercept-url` servlet path handling in Spring Security 7.

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 URL as follows:

```
<sec:intercept-url pattern="/servlet-path/endpoint/**" access="authenticated"/>
```

Use an `access` expression (or other supported authorization attributes) appropriate for your application.

Credit

The issue was identified and responsibly reported by [Apex](#), a Cantinas AppSec 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

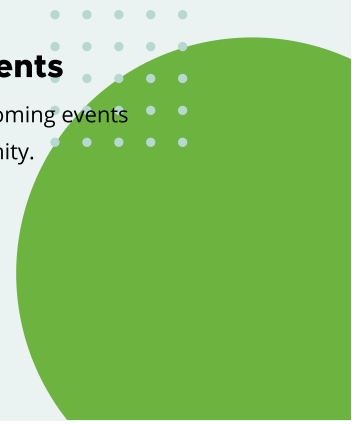
Tanzu Spring offers support and binaries for OpenJDK™, Spring, and Apache Tomcat® in one simple subscription.

[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.