

Spring Security Advisories

 [RSS feed](#)

CVE-2026-40976: Default security filter chain has no authorization rule with Actuator but without Health

CRITICAL | APRIL 23, 2026 | CVE-2026-40976

Description

In certain circumstances, Spring Boot's default web security is ineffective allowing unauthorized access to all endpoints. For an application to be vulnerable, it must:

- be a servlet-based web application
- have no Spring Security configuration of its own and rely on the default web security filter chain
- depend on spring-boot-actuator-autoconfigure
- not depend on spring-boot-health

If any of the above does not apply, the application is not vulnerable.

Affected Spring Products and Versions

Spring Boot:

- 4.0.0 - 4.0.5

Mitigation

Reporting a vulnerability

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

Affected version(s)	Fix version	Availability
4.0.x	4.0.6	OSS

No further mitigation steps are necessary.

References

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

History

- 2026-04-23: 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

Learn

Quickstart

Projects

Community

Events



Reference

- Event Driven
- Cloud
- Web Applications
- Serverless
- Batch

Courses

Get Certified

Blog

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

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.

