spring by VMware Tanzu

## 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 the Spring newsletter

Stay connected with the Spring newsletter

SUBSCRIBE