

Spring Security Advisories

[RSS feed](#)

CVE-2026-22748: Potential Security Misconfiguration when Using withIssuerLocation

MEDIUM | APRIL 20, 2026 | CVE-2026-22748

Description

When an application configures JWT decoding with `NimbusJwtDecoder` or `NimbusReactiveJwtDecoder`, it must configure an `OAuth2TokenValidator<Jwt>` separately, for example by calling `setJwtValidator`.

This is easy to miss when using `NimbusJwtDecoder#withIssuerLocation` or `NimbusReactiveJwtDecoder#withIssuerLocation`, which may be interpreted as adding issuer validation automatically.

Recent maintenance versions of `NimbusJwtDecoder#withIssuerLocation` and `NimbusReactiveJwtDecoder#withIssuerLocation` now add issuer validation by default.

Affected Spring Products and Versions

Spring Security:

- 6.3.0 - 6.3.14
- 6.4.0 - 6.4.14
- 6.5.0 - 6.5.9
- 7.0.0 - 7.0.4
- Older, unsupported versions are also affected.

Mitigation

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

Affected version(s)	Fix version	Availability
6.3.x	6.3.15	Enterprise Support Only
6.4.x	6.4.15	Enterprise Support Only
6.5.x	6.5.10	OSS
7.0.x	7.0.5	OSS

Note that if this upgrade causes you trouble due to unwanted issuer validation, you can change it to the earlier default in the following way:

```
@Bean
JwtDecoder jwtDecoder() {
    String issuer = "https://issuer.example.org";
```

Reporting a vulnerability

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

```

        .build();
    jwtDecoder.setOauth2TokenValidator(JwtValidators.createDefaults()); // set to t
    return jwtDecoder;
}

```

Credit

The issue was identified and responsibly reported by [Daniel Seiler](#).

References

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



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.