

Spring Security Advisories



CVE-2026-22751: Spring Security JdbcOneTimeTokenService allows a one-time token to authenticate multiple sessions

MEDIUM | APRIL 21, 2026 | CVE-2026-22751

Description

Applications that explicitly configure One-Time Token login with `JdbcOneTimeTokenService` are vulnerable to a Time-of-check Time-of-use (TOCTOU) race condition. An attacker with a valid one-time token can send concurrent requests to the authentication endpoint, allowing the single-use token to be consumed multiple times and establishing multiple authenticated sessions. The default `InMemoryOneTimeTokenService` is thread-safe and not affected by this vulnerability.

Affected Spring Products and Versions

Spring Security:

- 6.4.0 - 6.4.15
- 6.5.0 - 6.5.9
- 7.0.0 - 7.0.4

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
6.4.x	6.4.16	Commercial
6.5.x	6.5.10	OSS
7.0.x	7.0.5	OSS

Credit

The issue was identified and responsibly reported by Jinyeong Seol (@Seol-JY).

References

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

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
- 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



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.