

## Spring Security Advisories



# CVE-2026-40972: DevTools remote secret comparison is vulnerable to timing attacks

HIGH | APRIL 23, 2026 | CVE-2026-40972

## Description

An attacker on the same network as the remote application may be able to utilize a timing attack to discover information about the remote secret. In extreme circumstances this could result in the attacker determining the secret and uploading changed classes, thereby achieving remote code execution in the remote application.

## Affected Spring Products and Versions

Spring Boot:

- 4.0.0 - 4.0.5
- 3.5.0 - 3.5.13
- 3.4.0 - 3.4.15
- 3.3.0 - 3.3.18
- 2.7.0 - 2.7.32

Versions that are no longer supported are also affected.

## Mitigation

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

### Reporting a vulnerability

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



4.0.x	4.0.6	OSS
3.5.x	3.5.14	OSS
3.4.x	3.4.16	<a href="#">Enterprise Support Only</a>
3.3.x	3.3.19	<a href="#">Enterprise Support Only</a>
2.7.x	2.7.33	<a href="#">Enterprise Support Only</a>

No further mitigation steps are necessary.

## References

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





---

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.