

Spring Security Advisories



CVE-2026-22747: Unauthorized User Impersonation when Using X.509 Client Certificates

MEDIUM | APRIL 20, 2026 | CVE-2026-22747

Description

`SubjectX500PrincipalExtractor` does not correctly handle certain malformed X.509 certificate `CN` values, which can lead to reading the wrong value for the username. In a carefully crafted certificate, this can lead to an attacker impersonating another user.

Environmental Considerations

This component sits behind Spring Security's pre-authentication flow, which assumes the presented credentials have already been validated by a trusted upstream. Exploiting this issue therefore presupposes a compromise of that upstream trust. So while we recommend upgrading, this fix is better understood as defense-in-depth than as closing a standalone attack path.

Also note that this fix only addresses

`SubjectX500PrincipalExtractor` and not

`SubjectDnX509PrincipalExtractor`, a deprecated component.

Affected Spring Products and Versions

Spring Security:

Reporting a
vulnerability

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

Mitigation

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

Affected version(s)	Fix version	Availability
7.0.x	7.0.5	OSS

Credit

The issue was identified and responsibly reported by [Nikita Markevich](#).

References

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

Stay connected with the Spring newsletter



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.