spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2026-22746: User Attribute Enumeration when Using DaoAuthenticationProvider

LOW | APRIL 20, 2026 | CVE-2026-22746

Description

If an application is using the `UserDetails#isEnabled`, `#isAccountNonExpired`, or `#isAccountNonLocked` user attributes, to enable, expire, or lock users, then `DaoAuthenticationProvider`'s timing attack defense can be bypassed for users who are disabled, expired, or locked.

Affected Spring Products and Versions

Spring Security:

- 5.7.0 - 5.7.22
- 5.8.0 - 5.8.24
- 6.3.0 - 6.3.15
- 6.4.0 - 6.4.15
- 6.5.0 - 6.5.9
- 7.0.0 - 7.0.4
- Older, unsupported versions are also affected.

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
5.7.x	5.7.23	Enterprise Support Only
5.8.x	5.8.25	Enterprise Support Only
6.3.x	6.3.16	Enterprise Support Only
6.4.x	6.4.16	Enterprise Support Only
6.5.x	6.5.10	OSS
7.0.x	7.0.5	OSS

Note that this version also introduces a setter `DaoAuthenticationProvider#setAlwaysPerformAdditionalChecksOnUser`. In the event that this upgrade causes you trouble, you can set this value to `false`.

Credit

The issue was identified and responsibly reported by meverden.

References

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

History

- 2026-04-20: Initial vulnerability report published.

Get ahead Get support Upcoming events

spring by VMware Tanzu

certification to turbo-charge your progress.

Learn more

for OpenJDK™, Spring, and Apache Tomcat® in one simple subscription.

Learn more

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

spring by VMware Tanzu

spring by VMware Tanzu

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.