

## Spring Security Advisories



# CVE-2026-40967: VectorStore FilterExpression Converter injection

**HIGH | APRIL 27, 2026 | CVE-2026-40967**

## Description

In Spring AI, various FilterExpressionConverter implementations accept a filter expression object and translate them to specific vector store query languages. In several cases, keys and values are not properly escaped, leading to the ability to alter the query.

Only applications that use `VectorStore` implementations and pass user-supplied input as a `filterExpression` are affected.

## Affected Spring Products and Versions

### Spring AI:

- 1.0.0 - 1.0.x
- 1.1.0 - 1.1.x

## Mitigation

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

Affected version(s)	Fix version	Availability
1.0.x	1.0.6	OSS

## Reporting a vulnerability

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

1.1.x

1.1.5

OSS

No further mitigation steps are necessary.

## Credit

The issue was reported responsibly by

- Quan Le of Unit 515 from OPSWAT [@aleister1102](#)
- Cantina's AppSec agent, Apex (<https://www.cantina.security/>)
- [@Evil-Squirt1e](#)
- Bofei Chen [@qxyuan853](#)
- Andrew Orr at Tenable
- [@blindhacker99](#) - <https://x.com/ph0smet>
- ChenPeng [Ant Group]
- SharlongWen
- [@wo1enca1ca1](#)
- Meriem BELHORA [@MeryBelh](#)
- [@rockmelodies](#)
- Hyunwoo Kim ([@V4bel](#))
- Yu Bao [August829](#) - [yubao@paypal.com](mailto:yubao@paypal.com) - who works for paypal.com

## References

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

**Get ahead**

**Get support**

**Upcoming  
events**



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



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<sup>®</sup>, Apache Tomcat<sup>®</sup>, Apache Kafka<sup>®</sup>, Apache Cassandra<sup>™</sup>, and Apache Geode<sup>™</sup> are trademarks or registered trademarks of the Apache Software Foundation in the United States and/or other countries. Java<sup>™</sup>, Java<sup>™</sup> SE, Java<sup>™</sup> EE, and OpenJDK<sup>™</sup> are trademarks of Oracle and/or its affiliates. Kubernetes<sup>®</sup> is a registered trademark of the Linux Foundation in the United States and other countries. Linux<sup>®</sup> is the registered trademark of Linus Torvalds in the United States and other countries. Windows<sup>®</sup> and Microsoft<sup>®</sup> 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.