spring by VMware Tanzu

Spring Security Advisories

RSS feed

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 - 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

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