spring by VMware Tanzu

Spring Security Advisories

RSS feed

CVE-2026-40966: VectorStoreChatMemoryAdvisor conversation scoping can lead to cross-tenant memory exfiltration

MODERATE | APRIL 27, 2026 | CVE-2026-40966

Description

In Spring AI, an attacker can bypass conversation isolation and exfiltrate sensitive memory from other users' chat histories, including secrets and credentials, by injecting filter logic through `conversationId`.

Only applications that use `VectorStoreChatMemoryAdvisor` and pass user-supplied input as a conversationId 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.

Reporting a vulnerability

To report a security vulnerability for a project within the Spring portfolio, see the Security Policy

1.0.x	1.0.6	OSS
1.1.x	1.1.5	OSS

No further mitigation steps are necessary.

Credit

The issue was reported responsibly by

- Jinyeong Seol Seol-JY
- Cantina's AppSec agent, Apex (https://www.cantina.security)

References

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

Get the Spring newsletter

Stay connected with the Spring newsletter

SUBSCRIBE