VectorStoreChatMemoryAdvisor conversation scoping can lead to cross-tenant memory exfiltration

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40966
State	PUBLISHED
Assigner	vmware
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 08:16:01 UTC
Updated	2026-04-28 08:16:01 UTC
Description	In Spring AI, an attacker can bypass conversation isolation and exfiltrate sensitive memory from other users' chat histories,

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from security@vmware.com

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Problem Types: CWE-284 | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	security@vmware.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	CVSS	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
High

Privileges Required
None

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
None

Availability

None

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	VMware	Spring AI	affected 1.0.0 1.0.6 OSS	Not specified
CNA	VMware	Spring AI	affected 1.1.0 1.1.5 oss	Not specified

References

Reference	Source	Link	Tags
nvd.nist.gov/vuln-metrics/cvss/v3-calculator	security@vmware.com	nvd.nist.gov	
spring.io/security/cve-2026-40966	security@vmware.com	spring.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

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

There are currently no legacy QID mappings associated with this CVE.