Prompt Injection via Memory Poisoning in PromptChatMemoryAdvisor

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

Summary

CVE	CVE-2026-41713
State	PUBLISHED
Assigner	vmware
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-12 11:16:19 UTC
Updated	2026-05-12 19:25:06 UTC
Description	A malicious user could craft input that is stored in conversation memory and later interpreted by the model in an unintended

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from security@vmware.com

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

EPSS: 0.000330000 probability, percentile 0.098120000 (date 2026-05-12)

Problem Types: CWE-1336 | CWE-1336 CWE-1336 Improper Neutralization of Special Elements Used in a Template Engine

Version	Source	Type	Score	Severity	Vector
3.1	security@vmware.com	Secondary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N
3.1	CNA	CVSS	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

High

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vmware	Spring Ai	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	VMware	Spring AI	affected 1.0.0 1.0.7 oss	Not specified
CNA	VMware	Spring AI	affected 1.1.0 1.1.6 oss	Not specified

References

Reference	Source	Link	Tags
spring.io/security/cve-2026-41713	security@vmware.com	spring.io	Vendor Advisory
nvd.nist.gov/vuln-metrics/cvss/v3-calculator	security@vmware.com	nvd.nist.gov	US Government Resource
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: Ahmed Sekka (GitHub: https://github.com/ahmed-sekka) (en)

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