WeKnora: Tool Execution Hijacking via Ambigous Naming Convention In MCP client and Indirect Prompt Injection

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

Summary

CVE	CVE-2026-30856
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-07 17:15:53 UTC
Updated	2026-04-13 14:43:36 UTC
Description	WeKnora is an LLM-powered framework designed for deep document understanding and semantic retrieval. Prior to versio

Risk And Classification

Primary CVSS: v3.1 7.6 HIGH from nvd@nist.gov

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

EPSS: 0.000210000 probability, percentile 0.055960000 (date 2026-04-15)

Problem Types: CWE-706 | CWE-706 CWE-706: Use of Incorrectly-Resolved Name or Reference

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:L
3.1	security-advisories@github.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L
3.1	CNA	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tencent	Weknora	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tencent	WeKnora	affected < 0.3.0	Not specified

References

Reference	Source	Link	Tags
github.com/Tencent/WeKnora/security/advisories/GHSA-67q9-58vj-32qx	security-advisories@github.com	github.com	Exploit, Vendor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

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