MaxKB: Sandbox escape via ctypes and unhooked SYS_pkey_mprotect

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

Summary

CVE	CVE-2026-39421
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 01:16:04 UTC
Updated	2026-04-14 01:16:04 UTC
Description	MaxKB is an open-source AI assistant for enterprise. Versions 2.7.1 and below contain a sandbox escape vulnerability in th

Risk And Classification

Primary CVSS: v3.1 6.3 MEDIUM from security-advisories@github.com

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

EPSS: 0.000740000 probability, percentile 0.223570000 (date 2026-04-15)

Problem Types: CWE-94 | CWE-693 | CWE-693 CWE-693: Protection Mechanism Failure | CWE-94 CWE-94: Improper Control of Generation of Code ('Code Injection')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
3.1	CNA	DECLARED	6.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

Low

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	1Panel-dev	MaxKB	affected < 2.8.0	Not specified

References

Reference	Source	Link
github.com/1Panel-dev/MaxKB/commit/479701a4d2e6059506bad0057a66bed91abb5aef	security-advisories@github.com	github.com
github.com/1Panel-dev/MaxKB/releases/tag/v2.8.0	security-advisories@github.com	github.com
github.com/1Panel-dev/MaxKB/security/advisories/GHSA-9c6w-j7w5-3gf7	security-advisories@github.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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