MaxKB: Sandbox escape via LD_PRELOAD bypass

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

Summary

CVE	CVE-2026-39420
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 01:16:04 UTC
Updated	2026-04-20 17:35:22 UTC
Description	MaxKB is an open-source AI assistant for enterprise. In versions 2.7.1 and below, an incomplete sandbox protection mecha

Risk And Classification

Primary CVSS: v3.1 7.4 HIGH from nvd@nist.gov

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

EPSS: 0.001710000 probability, percentile 0.383520000 (date 2026-04-20)

Problem Types: CWE-78 | CWE-693 | CWE-693 CWE-693: Protection Mechanism Failure | CWE-78 CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.4	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:L
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

Changed

Confidentiality

Low

Integrity

Low

Availability

Low

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Maxkb	Maxkb	All	All	All	All

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/2d17b08e6b060329803754a05e806d0ddecf3fa8	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-7wgv-v2r3-7f7w	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.