



MaxKB: Sandbox Result Validation Bypass via Tool Output Spoofing

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-39419
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-14 02:16:05 UTC
Updated	2026-04-20 17:32:17 UTC
Description	MaxKB is an open-source AI assistant for enterprise. In versions 2.7.1 and below, an authenticated user can bypass sandb

Risk And Classification

Primary CVSS: v3.1 3.1 LOW from security-advisories@github.com

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

EPSS: 0.000520000 probability, percentile 0.162970000 (date 2026-04-20)

Problem Types: CWE-74 | CWE-290 | CWE-693 | CWE-74 CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') | CWE-693 CWE-693: Protection Mechanism Failure | CWE-290 CWE-290: Authentication Bypass by Spoofing

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

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

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	T
github.com/1Panel-dev/MaxKB/security/advisories/GHSA-f3c8-p474-xwfv	security-advisories@github.com	github.com	V
github.com/1Panel-dev/MaxKB/releases/tag/v2.8.0	security-advisories@github.com	github.com	R
github.com/1Panel-dev/MaxKB/commit/38c4cfeecd065293ede0437f6fa76cf0116591d25	security-advisories@github.com	github.com	P
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report