



# 1Panel-dev MaxKB MdPreview chat.ts cross site scripting

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

## Summary

<b>CVE</b>	CVE-2025-15632
<b>State</b>	PUBLISHED
<b>Assigner</b>	VulDB
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-13 10:16:10 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	A vulnerability has been found in 1Panel-dev MaxKB up to 2.4.2. Impacted is an unknown function of the file ui/src/chat.ts c

## Risk And Classification

**Primary CVSS:** v4.0 2 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000130000 probability, percentile 0.020800000 (date 2026-04-26)

**Problem Types:** CWE-79 | CWE-94 | CWE-79 Cross Site Scripting | CWE-94 Code Injection

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2	LOW	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	3.5	LOW	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	3.5	LOW	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.5	LOW	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	4		AV:N/AC:L/Au:S/C:N/I:P/A:N
2.0	CNA	DECLARED	4		AV:N/AC:L/Au:S/C:N/I:P/A:N/E:POC/RL:OF/RC:C

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Low

User Interaction

Passive

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

### CVSS v3.0 Breakdown

Attack Vector

Network

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	1Panel-dev	MaxKB	affected 2.4.0	Not specified
CNA	1Panel-dev	MaxKB	affected 2.4.1	Not specified
CNA	1Panel-dev	MaxKB	affected 2.4.2	Not specified
CNA	1Panel-dev	MaxKB	unaffected 2.5.0	Not specified

References

Reference	Source	Link	Tags
github.com/AnalogyC0de/public_exp/issues/28	cna@vuldb.com	github.com	
github.com/1Panel-dev/MaxKB/commit/7230daa5ec3e6574b6ede83dd48a4fbc0e70b8d8	cna@vuldb.com	github.com	
github.com/1Panel-dev/MaxKB/pull/4578	cna@vuldb.com	github.com	
github.com/1Panel-dev/MaxKB	cna@vuldb.com	github.com	
vuldb.com/submit/782265	cna@vuldb.com	vuldb.com	
github.com/1Panel-dev/MaxKB/releases/tag/v2.5.0	cna@vuldb.com	github.com	
vuldb.com/vuln/356967	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/356967/cti	cna@vuldb.com	vuldb.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

Vendor Comments And Credit

Discovery Credit

Discovery Credit

**CNA:** Ana10gy (VulDB User) (en)

**CNA:** VulDB CNA Team (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2026-04-11T00:00:00.000Z	Advisory disclosed
CNA	2026-04-11T02:00:00.000Z	VulDB entry created
CNA	2026-04-11T09:40:17.000Z	VulDB entry last update

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](#)