VDB-356967 · CVE-2025-15632 · SUBMIT #356967

1PANEL-DEV MAXKB UP TO 2.4.2 MDPREVIEW UI/SRC/CHAT.TS CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.2	$0-$5k	0.98

Summary

A vulnerability identified as problematic has been detected in 1Panel-dev MaxKB up to 2.4.2. The affected element is an unknown function of the file *ui/src/chat.ts* of the component *MdPreview*. Performing a manipulation results in cross site scripting. This vulnerability is reported as CVE-2025-15632. The attack is possible to be carried out remotely. Moreover, an exploit is present. You should upgrade the affected component. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Details

A vulnerability classified as problematic has been found in 1Panel-dev MaxKB up to 2.4.2. This affects some unknown functionality of the file *ui/src/chat.ts* of the component *MdPreview*. The manipulation with an unknown input leads to a cross site scripting vulnerability. CWE is classifying the issue as CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. This is going to have an impact on integrity.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2025-15632. The exploitability is told to be easy. It is possible to initiate the attack remotely. It demands that the victim is doing some kind of user interaction. Technical details and a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

The exploit is shared for download at github.com. It is declared as proof-of-concept. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Upgrading to version 2.5.0 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch 7230daa5ec3e6574b6ede83dd48a4fbc0e70b8d8 is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

Product

Vendor

- 1Panel-dev

Name

- MaxKB

Version

- 2.4.0
- 2.4.1
- 2.4.2

License

- open-source

Website

- Product: https://github.com/1Panel-dev/MaxKB/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 3.5
VulDB Meta Temp Score: 3.2

VulDB Base Score: 3.5

VulDB Temp Score: 3.2
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-94 / CWE-74
CAPEC: 🔒
ATT&CK: 🔒

Physical: No
Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: MaxKB 2.5.0
Patch: 7230daa5ec3e6574b6ede83dd48a4fbc0e70b8d8

Timeline

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/11/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: github.com
Status: Confirmed
Confirmation: 🔒

CVE: CVE-2025-15632 (🔒)
GCVE (CVE): GCVE-0-2025-15632
GCVE (VulDB): GCVE-100-356967
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/11/2026 09:40 AM
Changes: 04/11/2026 09:40 AM (62)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 20:3A6:179

Submit

Accepted

- Submit #782265: 1Panel-dev MaxKB <= v2.6.1 Stored XSS (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.