VDB-356966 · CVE-2026-6107 · SUBMIT #356966

1PANEL-DEV MAXKB UP TO 2.6.1 CHATHEADERSMIDDLEWARE CHAT_HEADERS_MIDDLEWARE.PY NAME CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.4	$0-$5k	1.33-

Summary

A vulnerability categorized as problematic has been discovered in 1Panel-dev MaxKB up to 2.6.1. Impacted is an unknown function of the file *apps/common/middleware/chat_headers_middleware.py* of the component *ChatHeadersMiddleware*. Such manipulation of the argument *Name* leads to cross site scripting. This vulnerability is documented as CVE-2026-6107. The attack can be executed remotely. There is not any exploit available. It is advisable to 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 was found in 1Panel-dev MaxKB up to 2.6.1. It has been rated as problematic. Affected by this issue is an unknown functionality of the file *apps/common/middleware/chat_headers_middleware.py* of the component *ChatHeadersMiddleware*. The manipulation of the argument `name` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to 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. Impacted is integrity.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-6107. The exploitation is known to be easy. The attack may be launched remotely. Successful exploitation requires user interaction by the victim. Technical details are known, but there is no available exploit. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Upgrading to version 2.8.0 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch 026a2d623e2aa5efa67c4834651e79d5d7cab1da 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.

Entry connected to this vulnerability is available at VDB-356965.

Product

Vendor

- 1Panel-dev

Name

- MaxKB

Version

- 2.6.0
- 2.6.1

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: 3.4

VulDB Base Score: 3.5
VulDB Temp Score: 3.4

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: 🔒
Status: Not defined
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: MaxKB 2.8.0
Patch: 026a2d623e2aa5efa67c4834651e79d5d7cab1da

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-2026-6107 (🔒)
GCVE (CVE): GCVE-0-2026-6107
GCVE (VulDB): GCVE-100-356966
See also: 🔒

Entry

Created: 04/11/2026 09:40 AM
Changes: 04/11/2026 09:40 AM (60)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 172:008:179

Submit

Accepted

- Submit #782263: 1Panel-dev MaxKB <= v2.6.1 Stored XSS (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.