VDB-356965 · CVE-2026-6106 · SUBMIT #356965

1PANEL-DEV MAXKB UP TO 2.2.1 PUBLIC CHAT INTERFACE STATIC_HEADERS_MIDDLEWARE.PY STATICHEADERSMIDDLEWARE NAME CROSS SITE SCRIPTING

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

3.2 | $0-$5k | 1.83

Summary

A vulnerability was found in 1Panel-dev MaxKB up to 2.2.1. It has been rated as problematic. This issue affects the function `StaticHeadersMiddleware` of the file *apps/common/middleware/static_headers_middleware.py* of the component *Public Chat Interface*. This manipulation of the argument *Name* causes cross site scripting. This vulnerability is registered as CVE-2026-6106. Remote exploitation of the attack is possible. Furthermore, an exploit is available. Upgrading the affected component is advised. 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 2.2.1. It has been declared as problematic. Affected by this vulnerability is the function `StaticHeadersMiddleware` of the file *apps/common/middleware/static_headers_middleware.py* of the component *Public Chat Interface*. The manipulation of the argument `name` with an unknown input leads to a cross site scripting vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect integrity.

The advisory is shared at github.com. This vulnerability is known as CVE-2026-6106. The exploitation appears to be easy. The attack can be launched remotely. It demands that the victim is doing some kind of user interaction. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1059.007 for this issue.

It is possible to download the exploit 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 2.8.0 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.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-21686). Similar entry is available at VDB-356966.

Product

Vendor

- 1Panel-dev

Name

- MaxKB

Version

- 2.2.0
- 2.2.1

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: 3.2

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 2.8.0
Patch: 026a2d623e2aa5efa67c4834651e79d5d7cab1da

Timeline

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/12/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: github.com
Status: Confirmed
Confirmation: 🔒

CVE: CVE-2026-6106 (🔒)
GCVE (CVE): GCVE-0-2026-6106
GCVE (VulDB): GCVE-100-356965
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/11/2026 09:40 AM
Updated: 04/12/2026 01:07 AM
Changes: 04/11/2026 09:40 AM (64), 04/11/2026 10:25 AM (1), 04/12/2026 01:07 AM (1)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 52:0E4:179

Submit

Accepted

- Submit #781810: 1Panel-dev MaxKB <= v2.2.1 Stored XSS (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.