VDB-356968 · CVE-2026-6108 · SUBMIT #356968

1PANEL-DEV MAXKB UP TO 2.6.1 MODEL CONTEXT PROTOCOL NODE BASE_MCP_NODE.PY EXECUTE OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	1.97-

Summary

A vulnerability labeled as critical has been found in 1Panel-dev MaxKB up to 2.6.1. The impacted element is the function `execute` of the file *apps/application/flow/step_node/mcp_node/impl/base_mcp_node.py* of the component *Model Context Protocol Node*. Executing a manipulation can lead to os command injection. This vulnerability appears as CVE-2026-6108. The attack may be performed from remote. In addition, an exploit is available. The affected component should be upgraded. 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 critical was found in 1Panel-dev MaxKB up to 2.6.1. This vulnerability affects the function `execute` of the file *apps/application/flow/step_node/mcp_node/impl/base_mcp_node.py* of the component *Model Context Protocol Node*. The manipulation with an unknown input leads to a os command injection vulnerability. The CWE definition for the vulnerability is CWE-78. The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability was named CVE-2026-6108. The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1202.

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 eliminates this vulnerability.

See VDB-161782, VDB-216445, VDB-218397 and VDB-233476 for similar entries.

Product

Vendor

- 1Panel-dev

Name

- MaxKB

Version

- 2.6.0
- 2.6.1

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Os command injection
CWE: CWE-78 / CWE-77 / 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: 🔒

Timeline

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

Sources

Advisory: github.com
Status: Confirmed

CVE: CVE-2026-6108 (🔒)
GCVE (CVE): GCVE-0-2026-6108
GCVE (VulDB): GCVE-100-356968
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/11/2026 09:40 AM
Changes: 04/11/2026 09:40 AM (58)
Complete: 🔍
Submitter: Ana10gy
Cache ID: 52:BD3:179

Submit

Accepted

- Submit #782279: 1Panel-dev MaxKB <= v2.6.1 Remote Code Execution (by Ana10gy)

Discussion

No comments yet. Languages: en.

Please log in to comment.