COMMUNITY CONTENT

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

Title	1Panel-dev MaxKB <= v2.6.1 Remote Code Execution
Description	MaxKB is vulnerable to Remote Code Execution (RCE) due to improper validation placement in its Model Context Protocol (MCP) node implementation. Although the application implements a whitelist to restrict MCP transport types to safe values ('sse' and 'streamable_http'), this validation is only enforced on the tool-listing API endpoint. It is bypassed entirely during workflow application saving and execution. An authenticated user can inject arbitrary transport configurations (such as stdio with OS commands) via the application edit endpoint. When the workflow is subsequently triggered, the unsanitized configuration is passed directly to the MultiServerMCPClient, resulting in arbitrary shell command execution on the host server.
Source	https://github.com/AnalogyC0de/public_exp/issues/30
User	Ana1ogy (UID 93358)
Submission	03/18/2026 01:49 PM (25 days ago)
Moderation	04/11/2026 09:35 AM (24 days later)
Status	Approved
VulDB entry	[1Panel-dev MaxKB up to 2.6.1 Model Context Protocol Node base_mcp_node.py execute os command injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling