COMMUNITY CONTENT

Submit #792655: AstrBotDevs AstrBot 4.22.1 Arbitrary Command Execution

Title	AstrBotDevs AstrBot 4.22.1 Arbitrary Command Execution
Description	AstrBot versions up to and including 4.22.1 allow authenticated dashboard users to add MCP (Model Context Protocol) server configurations via the /api/tools/mcp/add endpoint. The MCP server configuration includes a command field specifying the executable to launch and an args field for command-line arguments. These values are passed directly to subprocess execution without any validation or restriction, allowing an attacker with dashboard access to execute arbitrary system commands.
Source	https://github.com/AstrBotDevs/AstrBot/issues/7169
User	Yu_Bao (UID 89348)
Submission	03/30/2026 05:32 AM (13 days ago)
Moderation	04/11/2026 10:50 AM (12 days later)
Status	Accepted
VulDB entry	[AstrBotDevs AstrBot up to 4.22.1 MCP Endpoint tools.py add_mcp_server command 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