COMMUNITY CONTENT

Home › Submit › 795355

Submit #795355: chatboxai chatbox 1.20.0 Arbitrary Command Execution

Title	chatboxai chatbox 1.20.0 Arbitrary Command Execution
Description	Chatbox v1.20.0 contains an arbitrary command execution vulnerability in the MCP (Model Context Protocol) stdio transport IPC handler. The mcp:stdio-transport:create IPC channel accepts command, args, and env parameters directly from the renderer process and spawns a child process via StdioClientTransport without any validation, sanitization, or command allowlisting. Since ipcRenderer.invoke is directly exposed via the Electron context bridge (see chatbox_02), any JavaScript running in the renderer context can execute arbitrary system commands with the full privileges of the Electron main process.
Source	https://github.com/chatboxai/chatbox/issues/3627
User	Yu_Bao (UID 89348)
Submission	04/02/2026 11:03 AM (11 days ago)
Moderation	04/12/2026 06:30 AM (10 days later)
Status	Accepted
VulDB entry	356993 [chatboxai chatbox up to 1.20.0 Model Context Protocol Server Management System ipc-stdio-transport.ts StdioClientTransport args/env 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