kleneway / **awesome-cursor-mpc-server** Public

Code | Issues 6 | **Pull requests 4** | Actions | Projects | Security and quality

fix: prevent command injection in code-review tool #14

Open **123mutouren321414** wants to merge 1 commit into `kleneway:main` from `123mutouren321414:fix-command-inj…`

Conversation 0 | Commits 1 | Checks 0 | Files changed 1

123mutouren321414 commented 3 weeks ago

This patch fixes a command injection vulnerability in the code-review tool caused by unsafe use of child_process.execSync with interpolated user input.

The original implementation constructed a shell command using a user-controlled folderPath value, which could allow execution of arbitrary commands via shell metacharacters.

This change replaces execSync with execFileSync and passes arguments as an array, ensuring that user input is treated strictly as data rather than being interpreted by a shell.

The fix preserves the original functionality while eliminating the injection risk.

`fix: prevent command injection in code-review tool` … `a7ac7ba`

123mutouren321414 mentioned this pull request 3 weeks ago

Command Injection in MCP Server awesome-cursor-mpc-server due to execSync() with unsanitized folderPath #6

Open

Reviewers

No reviews

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

1 participant