fix: prevent command injection by replacing exec with execFile #5

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

Conversation Commits 1 Checks Files changed

123mutouren321414 commented 3 weeks ago

Replaced child_process.exec with execFile to avoid shell invocation.

Previously, user-controlled input could be interpolated into a command string and executed via a shell, leading to potential command injection.

This change uses argument arrays with execFile, ensuring inputs are treated as data rather than shell commands.

Also removed shell-based output chaining (&& cat), and standardized the return value to the output file path to match downstream usage.

`fix: prevent command injection by replacing exec with execFile` ··· `a2a508d`

123mutouren321414 mentioned this pull request 3 weeks ago

Command Injection in MCP Server mcp-code-review-server due to exec() with unsanitized specificFiles #4

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