[WIP] Fix security vulnerability: Command injection in magento2-dev-mcp #5

Merged **peterjaap** merged 2 commits into `master` from `copilot/fix-command-injection-vul…` last month

Copilot AI commented last month • edited — Contributor

- [x] Refactor `executeMagerun2Command` in `src/index.ts` to accept `args: string[]` instead of a command string
- [x] Use `execFile` (via `execFileAsync`) for local execution to avoid shell entirely
- [x] Use `shellQuote` for each arg when building Docker wrapper command strings
- [x] Separate flag names from their user-controlled values into distinct array elements (`--flag`, value)
- [x] Update all 28 callers of `executeMagerun2Command` to pass argument arrays
- [x] Run build to verify changes compile correctly
- [x] Run CodeQL security scan: 0 alerts found

▶ Original prompt

- Fixes **Security Vulnerability: Command Injection in multiple magento2-dev-mcp tools due to unsafe use of child_process.execAsync** #4

🔒 GitHub Advanced Security automatically protects Copilot coding agent pull requests. You can protect all pull requests by enabling Advanced Security for your repositories. Learn more about Advanced Security.

`Initial plan` `1dac674`

Copilot AI assigned **Copilot** and **peterjaap** last month

Copilot started work on behalf of **peterjaap** last month

View session

`fix: prevent command injection by using execFile and shellQuote for m…` `235f93b`

…

peterjaap marked this pull request as ready for review last month

peterjaap merged commit **`aa1ffcc`** into `master` last month

Copilot stopped work on behalf of **peterjaap** due to an error last month

The session was cancelled by the user.

Reviewers

No reviews

Assignees

peterjaap

Copilot

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

Security Vulnerability: Command Injection in multiple magento2-dev-mcp tools due to unsafe use of child_proce…

2 participants