PrefectHQ / **fastmcp** Public

Code | Issues 220 | **Pull requests 21** | Discussions | Actions | Projects

fix: validate server names in install commands #3522

Merged **jlowin** merged 2 commits into `main` from `fix/sanitize-install-server-name` on Mar 15

Conversation | Commits 2 | Checks | Files changed

jlowin commented on Mar 15 — Member

Server names passed to `fastmcp install` are used as subprocess arguments to CLI tools like `claude` and `gemini`. On Windows, these tools often resolve to `.cmd` wrappers that run through `cmd.exe`, where shell metacharacters in arguments can be interpreted. This adds validation at the shared install entry point to restrict server names to alphanumeric characters, hyphens, underscores, dots, and spaces.

👍 1

`fix: validate server names in install commands` cc2e3ab

jlowin added the bug label on Mar 15

jlowin mentioned this pull request on Mar 15

Harden install commands against special characters #2371

Closed

marvin-context-protocol Bot added security cli labels on Mar 15

chatgpt-codex-connector Bot reviewed on Mar 15

View reviewed changes

chatgpt-codex-connector Bot left a comment

💡 Codex Review

Here are some automated review suggestions for this pull request.

Reviewed commit: `cc2e3ab11f`

▶ ℹ️ About Codex in GitHub

`src/fastmcp/cli/install/shared.py` Outdated

```
123  144                )
124  145                name = file.stem
125  146
     147  +     validate_server_name(name)
```

chatgpt-codex-connector Bot on Mar 15

P2 Scope server-name validation to shell-backed install paths

Calling `validate_server_name` unconditionally in `process_common_args` makes every install backend reject names containing characters like `(` or `&`, but some backends (notably Cursor/Goose deeplinks) already URL-encode names with `quote(..., safe='')` and do not pass them through a shell. This introduces a regression where previously supported names such as `"my server (test)"` or `"test&evil=true"` now exit early for `cursor` / `goose` / `mcp-json` flows even though those paths can safely carry them, so validation should be limited to shell-backed commands (e.g. claude/gemini) or made backend-specific.

Useful? React with 👍 / 👎.

`Scope validation to shell-backed install paths only` `a40e6ad`

jlowin merged commit **`b2d4cc9`** into `main` on Mar 15

7 checks passed

View details

jlowin deleted the `fix/sanitize-install-server-name` branch 2 months ago

jlowin added a commit that referenced this pull request on Mar 30

`Publish docs for v3.2.0 (#3713)` ··· `3a9717e`

Reviewers

chatgpt-codex-connector[bot]

Assignees

No one assigned

Labels

bug cli security

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

1 participant