fix: prevent command injection by replacing child_process.exec with e… #2

Merged **silesmo** merged 1 commit into `Nor2-io:main` from `123mutouren321414:fix-command-inj…` 2 weeks ago

123mutouren321414 commented last month — Contributor

…xecFile

This change replaces unsafe uses of `child_process.exec` with `execFile` and passes command arguments as arrays instead of interpolated shell command strings.

Previously, several tools constructed shell command strings using user-controlled parameters such as `path`, `openApiPath`, `name`, `version`, and `basePath`, and executed them via `child_process.exec`. Because `exec` invokes commands through a system shell, specially crafted input could potentially be interpreted as additional commands, leading to command injection.

This update:

1. replaces `child_process.exec` with `execFile`
2. passes command arguments as arrays instead of constructing shell command strings
3. safely handles optional parameters (such as `path`) when building argument arrays
4. preserves the existing functionality and CLI behavior

By avoiding shell interpretation of user-controlled input, this change prevents potential command injection vulnerabilities while maintaining the original tool behavior.

`fix: prevent command injection by replacing child_process.exec with e…` `2b1864f`

…

123mutouren321414 mentioned this pull request last month

Security Vulnerability: Command Injection in multiple heim-mcp tools due to unsafe use of child_process.exec #1

Closed

silesmo approved these changes 2 weeks ago

View reviewed changes

silesmo left a comment — Member

Thanks for your contribution!

silesmo merged commit `c321d8a` into `Nor2-io:main` 2 weeks ago

Reviewers

silesmo ✓

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

---

2 participants