New issue

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

Closed

123mutouren321414 opened last month Contributor

Summary

The MCP server *heim-mcp* is vulnerable to command injection due to unsafe use of child_process.exec with user-controlled input in the ***new_heim_application***, ***deploy_heim_application***, and ***deploy_heim_application_to_cloud*** tools.

Affected Versions

<= 0.1.3

Vulnerable Code

deploy_heim_application:
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L121
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L104-L109
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L118-L120
deploy_heim_application_to_cloud:
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L165
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L147-L152
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L161-L164
new_heim_application:
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L65-L72
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L14-L53
https://github.com/Nor2-io/heim-mcp/blob/main/src/tools.ts#L62-L64

Details

The MCP server heim-mcp constructs command strings using user-supplied parameters and executes them via child_process.exec in multiple tools. Because exec invokes commands through a system shell, specially crafted input containing shell metacharacters (such as ;, &, or |) may be interpreted as additional commands rather than treated as data.
For example, an attacker could supply a malicious value in path to inject arbitrary shell commands, which would then be executed with the privileges of the MCP server process.
The vulnerability results from shell-based command execution combined with direct interpolation of untrusted input. In MCP environments, LLM-generated tool parameters influenced by external content may trigger execution of injected commands without direct local user interaction.

Impact

Successful exploitation allows attackers to execute arbitrary commands on the server hosting the MCP service. This may allow attackers to execute commands, access sensitive data, or modify the host environment depending on the privileges of the MCP server.

Recommendation

1. Don't use exec. Use execFile instead, which pins the command and provides the arguments as array elements.
2. Apply strict input validation to all tool parameters exposed to MCP clients, especially path, openApiPath, name, version, language, and basePath parameters.
3. Use parameter separation with proper escaping to prevent shell command injection.

PoC

See the attached files:
heim-mcp_bug.pdf

123mutouren321414 last month Contributor Author •••

#2

123mutouren321414 last month Contributor Author •••

Hi **@silesmo**,

I recently reported a potential command injection vulnerability in this project and also submitted a PR with a minimal fix.

Could you please take a look when you have time?

I have also sent an email notification in case GitHub notifications were missed.

Thanks a lot!

123mutouren321414 3 weeks ago Contributor Author •••

security_advisory:

heim-mcp_security_advisory.pdf

silesmo 2 weeks ago Member •••

Thanks for reporting the issue and submitting a PR with the fix! Resolved with the merge of #2

silesmo closed this as completed 2 weeks ago

Metadata

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

No branches or pull requests

Participants