COMMUNITY CONTENT

Home › Submit › 784862

Submit #784862: Nor2-io heim-mcp <=0.1.3 Command Injection

Title	Nor2-io heim-mcp <=0.1.3 Command Injection
Description	A command injection vulnerability exists in Nor2-io/heim-mcp due to unsafe use of child_process.exec when constructing Heim CLI commands with user-controlled input. Successful exploitation allows attackers to execute arbitrary shell commands with the privileges of the MCP server process. The following MCP tools construct command strings using user-supplied parameters and execute them via child_process.exec: • new_heim_application: interpolates path, openApiPath, name, version, language, and basePath parameters • deploy_heim_application: interpolates path parameter • deploy_heim_application_to_cloud: interpolates path parameter 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.
Source	⚠ https://github.com/Nor2-io/heim-mcp/issues/1
User	Yinci Chen (UID 94659)
Submission	03/21/2026 09:57 AM (16 days ago)
Moderation	04/05/2026 03:30 PM (15 days later)
Status	Accepted
VulDB entry	353384 [Nor2-io heim-mcp up to 0.1.3 new_heim_application src/tools.ts registerTools os command injection]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling