New issue

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

Closed #5

Assignees

123mutouren321414 opened last month

Summary

The MCP server ***magento2-dev-mcp*** is vulnerable to command injection due to unsafe use of child_process.execAsync with user-controlled input in multiple tools.

Affected Versions

<= 1.0.2

Vulnerable Code

https://github.com/elgentos/magento2-dev-mcp/blob/master/src/index.ts#L386-L387
https://github.com/elgentos/magento2-dev-mcp/blob/master/src/index.ts#L377-L383
https://github.com/elgentos/magento2-dev-mcp/blob/master/src/index.ts#L388

Details

The MCP server magento2-dev-mcp constructs command strings using user-supplied parameters and executes them via child_process.execAsync in multiple tools. Because execAsync 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 *key* 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 key, type, path, value, query, event, vendorNamespace, moduleName, authorName, authorEmail, description, languages, themes, storeId, job, and group parameters.
3. Use parameter separation with proper escaping to prevent shell command injection.

PoC

See the attached files:
magento2-dev-mcp_bug.pdf

👀 1

123mutouren321414 last month Author •••

Hi **@peterjaap** ,

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?

Thanks a lot!

peterjaap assigned Copilot and peterjaap last month

Copilot mentioned this last month

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

peterjaap last month Contributor •••

I'll let AI fix your AI generated report

peterjaap closed this as completed in #5 last month

123mutouren321414 3 weeks ago Author •••

magento2-dev-mcp_security_advisory.pdf

Metadata

Assignees

Copilot

peterjaap

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode

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

elgentos/magento2-dev-mcp

Participants