COMMUNITY CONTENT

Home › Submit › 784864

Submit #784864: elgentos magento2-dev-mcp <=1.0.2 Command Injection

Title elgentos magento2-dev-mcp <=1.0.2 Command Injection

Description A command injection vulnerability exists in elgentos/magento2-dev-mcp due to unsafe use of child_process.execAsync when constructing Magerun2 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.execAsync:

- config-show: interpolates path, scope, and scopeId parameters
- config-set: interpolates path, value, scope, and scopeId parameters
- config-store-get: interpolates path and storeId parameters
- config-store-set: interpolates path, value, and storeId parameters
- cache-view: interpolates key and type parameters
- db-query: interpolates query parameter
- dev-module-observer-list: interpolates event parameter
- dev-module-create: interpolates vendorNamespace, moduleName, authorName, authorEmail, and description parameters
- setup-static-content-deploy: interpolates languages and themes parameters
- sys-url-list: interpolates storeId parameter
- sys-cron-run: interpolates job and group parameters

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.

Source https://github.com/elgentos/magento2-dev-mcp/issues/4

User Yinxi Chen (UID 94659)

Submission 03/21/2026 09:59 AM (16 days ago)

Moderation 04/05/2026 03:58 PM (15 days later)

Status Pending

VulDB entry [elgentos magento2-dev-mcp up to 1.0.2 src/index.ts executeMagerun2Command 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