VDB-355395 · CVE-2026-5603 · GCVE-100-355395

ELGENTOS MAGENTO2-DEV-MCP UP TO 1.0.2 SRC/INDEX.TS EXECUTEMAGERUN2COMMAND OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	1.80

Summary

A vulnerability was found in elgentos magento2-dev-mcp up to 1.0.2. It has been classified as critical. The impacted element is the function `executeMagerun2Command` of the file *src/index.ts*. Performing a manipulation results in os command injection. This vulnerability is known as CVE-2026-5603. Attacking locally is a requirement. Furthermore, an exploit is available. To fix this issue, it is recommended to deploy a patch.

Details

A vulnerability, which was classified as critical, was found in elgentos magento2-dev-mcp up to 1.0.2. This affects the function `executeMagerun2Command` of the file *src/index.ts*. The manipulation with an unknown input leads to a os command injection vulnerability. CWE is classifying the issue as CWE-78. The product constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2026-5603. The exploitability is told to be easy. Attacking locally is a requirement. Technical details and a public exploit are known. The attack technique deployed by this issue is T1202 according to MITRE ATT&CK.

The exploit is shared for download at github.com. It is declared as proof-of-concept.

Applying the patch aa1ffcc0aea1b212c69787391783af27df15ae9d is able to eliminate this problem. The bugfix is ready for download at github.com.

Similar entries are available at VDB-169422, VDB-222729, VDB-344765 and VDB-348559.

Product

Type

- E-Commerce Management Software

Vendor

- elgentos

Name

- magento2-dev-mcp

Version

- 1.0.0
- 1.0.1
- 1.0.2

License

- open-source

Website

- Product: https://github.com/elgentos/magento2-dev-mcp/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 4.8

VulDB Base Score: 5.3
VulDB Temp Score: 4.8
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Os command injection
CWE: CWE-78 / CWE-77 / CWE-74
CAPEC: 🔒
ATT&CK: 🔒

Physical: Partially
Local: Yes
Remote: No

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Patch
Status: 🔍

0-Day Time: 🔒

Patch: aa1ffcc0aea1b212c69787391783af27df15ae9d

Timeline

04/05/2026		Advisory disclosed
04/05/2026	+0 days	VulDB entry created
04/05/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: github.com
Status: Confirmed
Confirmation: 🔒

CVE: CVE-2026-5603 (🔒)
GCVE (CVE): GCVE-0-2026-5603
GCVE (VulDB): GCVE-100-355395
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 04:03 PM
Changes: 04/05/2026 04:03 PM (60)

Complete: 🔍

Submitter: Yinci Chen

Cache ID: 172:ECF:179

Submit

Accepted

- Submit #784864: elgentos magento2-dev-mcp <=1.0.2 Command Injection (by Yinci Chen)

Discussion

No comments yet. Languages: en.

Please log in to comment.