VDB-355281 · CVE-2026-5528 · GCVE-100-355281

MOUSSAABBADLA CODE-SCREENSHOT-MCP UP TO 0.1.0 HTTP INTERFACE OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
5.7	$0-$5k	2.07-

Summary

A vulnerability has been found in MoussaabBadla code-screenshot-mcp up to 0.1.0 and classified as critical. This vulnerability affects unknown code of the component *HTTP Interface*. Performing a manipulation results in os command injection. This vulnerability is identified as CVE-2026-5528. The attack can be initiated remotely. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability was found in MoussaabBadla code-screenshot-mcp up to 0.1.0. It has been classified as critical. This affects an unknown part of the component *HTTP Interface*. 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.

The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2026-5528. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details are unknown but a public exploit is available. MITRE ATT&CK project uses the attack technique T1202 for this issue.

The exploit is shared for download at github.com. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Entries connected to this vulnerability are available at VDB-152034, VDB-160017, VDB-169011 and VDB-196575.

Product

Vendor

- MoussaabBadla

Name

- code-screenshot-mcp

Version

- 0.1.0

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 6.3
VulDB Meta Temp Score: 5.7

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
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: No
Local: No
Remote: Yes

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

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

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

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5528 (🔒)
GCVE (CVE): GCVE-0-2026-5528
GCVE (VulDB): GCVE-100-355281
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 08:29 AM
Changes: 04/04/2026 08:29 AM (55)
Complete: 🔍
Submitter: BruceJin
Cache ID: 172:FB3:179

Submit

Accepted

- Submit #782064: MoussaabBadla code-screenshot-mcp 0.1.0 Command Injection (by BruceJin)

Discussion

No comments yet. Languages: en.

Please log in to comment.