VDB-355394 · CVE-2026-5602 · GCVE-100-355394

NOR2-IO HEIM-MCP UP TO 0.1.3 NEW_HEIM_APPLICATION SRC/TOOLS.TS REGISTERTOOLS OS COMMAND INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
4.8	$0-$5k	1.74

Summary

A vulnerability was found in Nor2-io heim-mcp up to 0.1.3 and classified as critical. The affected element is the function `registerTools` of the file *src/tools.ts* of the component *new_heim_application/deploy_heim_application/deploy_heim_application_to_cloud*. Such manipulation leads to os command injection. This vulnerability is traded as CVE-2026-5602. An attack has to be approached locally. Furthermore, there is an exploit available. A patch should be applied to remediate this issue. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Details

A vulnerability, which was classified as critical, has been found in Nor2-io heim-mcp up to 0.1.3. Affected by this issue is the function `registerTools` of the file *src/tools.ts* of the component *new_heim_application/deploy_heim_application/deploy_heim_application_to_cloud*. The manipulation with an unknown input leads to a os command injection vulnerability. Using CWE to declare the problem leads to 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. Impacted is confidentiality, integrity, and availability.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-5602. The exploitation is known to be easy. Local access is required to approach this attack. Technical details as well as a public exploit are known. This vulnerability is assigned to T1202 by the MITRE ATT&CK project.

The exploit is available at github.com. It is declared as proof-of-concept. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Applying the patch c321d8af25f77668781e6ccb43a1336f9185df37 is able to eliminate this problem. The bugfix is ready for download at github.com.

Product

Type

- Artificial Intelligence Software

Vendor

- Nor2-io

Name

- heim-mcp

Version

- 0.1.0
- 0.1.1
- 0.1.2
- 0.1.3

License

- open-source

Website

- Product: https://github.com/Nor2-io/heim-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: c321d8af25f77668781e6ccb43a1336f9185df37

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-2026-5602 (🔒)
GCVE (CVE): GCVE-0-2026-5602
GCVE (VulDB): GCVE-100-355394
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 04/05/2026 03:35 PM
Changes: 04/05/2026 03:35 PM (61)
Complete: 🔍

Submitter: Yinci Chen

Cache ID: 20:78D:179

Submit

Accepted

- Submit #784862: Nor2-io heim-mcp <=0.1.3 Command Injection (by Yinci Chen)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa