VDB-307365 · CVE-2025-4261 · ISSUE 50

GAIR-NLP FACTOOL UP TO 3F3914BC090B644BE044B7E0005113C135D8B20F TOOL.PY RUN_SINGLE CODE INJECTION

A vulnerability was found in GAIR-NLP factool up to 3f3914bc090b644be044b7e0005113c135d8b20f. It has been classified as critical. This affects the function `run_single` of the file *factool/factool/math/tool.py*. The manipulation with an unknown input leads to a code injection vulnerability. CWE is classifying the issue as CWE-94. The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. This is going to have an impact on confidentiality, integrity, and availability.

The weakness was published with StarMap Team of Legendsec at QI-ANXIN Group as *50*. The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2025-4261. The exploitability is told to be easy. An attack has to be approached locally. Technical details and a public exploit are known. MITRE ATT&CK project uses the attack technique T1059 for this issue.

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

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

Product

Vendor

- GAIR-NLP

Name

- factool

Version

- 3f3914bc090b644be044b7e0005113c135d8b20f

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA CVSS-B Score: 🔒
CNA CVSS-BT Score: 🔒
CNA Vector: 🔒

CVSSv3

VulDB Meta Base Score: 5.3
VulDB Meta Temp Score: 5.0

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

CNA Base Score: 5.3
CNA Vector: 🔒

CVSSv2

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

Exploiting

Class: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
CAPEC: 🔒
ATT&CK: 🔒

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: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/04/2025		Advisory disclosed
05/04/2025	+0 days	VulDB entry created
05/05/2025	+1 days	VulDB entry last update

Sources

Advisory: 50
Organization: StarMap Team of Legendsec at QI-ANXIN Group
Status: Not defined

CVE: CVE-2025-4261 (🔒)
GCVE (CVE): GCVE-0-2025-4261
GCVE (VulDB): GCVE-100-307365
scip Labs: https://www.scip.ch/en/?labs.20161013

Entry

Created: 05/04/2025 08:12 PM
Updated: 05/05/2025 04:32 PM
Changes: 05/04/2025 08:12 PM (57), 05/05/2025 07:57 AM (30), 05/05/2025 04:32 PM (1)
Complete: 🔍

Submitter: ybdesire
Committer: ybdesire
Cache ID: 5:B83:101

Submit

Accepted

- Submit #562942: GAIR-NLP factool 0.0 Code Injection (by ybdesire)

Discussion

No comments yet. Languages: en.

Please log in to comment.