VDB-356970 · CVE-2026-6110 · ISSUE 1933

FOUNDATIONAGENTS METAGPT UP TO 0.8.1 TREE-OF-THOUGHT SOLVER METAGPT/STRATEGY/TOT.PY GENERATE_THOUGHTS CODE INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.6	$0-$5k	2.29-

Summary

A vulnerability described as critical has been identified in FoundationAgents MetaGPT up to 0.8.1. This impacts the function `generate_thoughts` of the file *metagpt/strategy/tot.py* of the component *Tree-of-Thought Solver*. The manipulation results in code injection. This vulnerability is known as CVE-2026-6110. It is possible to launch the attack remotely. Furthermore, an exploit is available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability, which was classified as critical, was found in FoundationAgents MetaGPT up to 0.8.1. Affected is the function `generate_thoughts` of the file *metagpt/strategy/tot.py* of the component *Tree-of-Thought Solver*. 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 advisory is available at github.com. This vulnerability is traded as CVE-2026-6110. The exploitability is told to be easy. It is possible to launch the attack remotely. The exploitation doesn't require any form of authentication. Technical details and a public exploit are known. This vulnerability is assigned to T1059 by the MITRE ATT&CK project.

The exploit is shared for download at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

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

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-21696). Similar entry is available at VDB-342028.

Product

Vendor

- FoundationAgents

Name

- MetaGPT

Version

- 0.8.0
- 0.8.1

Website

- Product: https://github.com/FoundationAgents/MetaGPT/

CPE 2.3

- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3
VulDB Temp Score: 6.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
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

04/11/2026		Advisory disclosed
04/11/2026	+0 days	VulDB entry created
04/12/2026	+1 days	VulDB entry last update

Sources

Product: github.com

Advisory: 1933
Status: Not defined
Confirmation: 🔒

CVE: CVE-2026-6110 (🔒)
GCVE (CVE): GCVE-0-2026-6110
GCVE (VulDB): GCVE-100-356970
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/11/2026 09:54 AM
Updated: 04/12/2026 06:14 AM
Changes: 04/11/2026 09:54 AM (59), 04/12/2026 06:14 AM (1)
Complete: 🔍
Submitter: Eric-d
Cache ID: 52:E32:179

Submit

Accepted

- Submit #791761: FoundationAgents MetaGPT 0.8.1 Code Injection (CWE-94) (by Eric-d)

Discussion

No comments yet. Languages: en.

Please log in to comment.