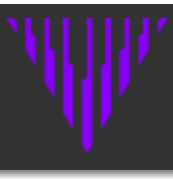

VDB-356969 · CVE-2026-6109 · ISSUE 1932

FOUNDATIONAGENTS METAGPT UP TO 0.8.1 MINEFLAYER HTTP API INDEX.JS EVALUATECODE CROSS-SITE REQUEST FORGERY

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.9	$0-$5k	1.77-

Summary

A vulnerability marked as problematic has been reported in FoundationAgents MetaGPT up to 0.8.1. This affects the function `evaluateCode` of the file *metagpt/environment/minecraft/mineflayer/index.js* of the component *Mineflayer HTTP API*. The manipulation leads to cross-site request forgery. This vulnerability is traded as CVE-2026-6109. It is possible to initiate the attack remotely. Furthermore, there is an exploit 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 problematic, has been found in FoundationAgents MetaGPT up to 0.8.1. This issue affects the function `evaluateCode` of the file *metagpt/environment/minecraft/mineflayer/index.js* of the component *Mineflayer HTTP API*. The manipulation with an unknown input leads to a cross-site request forgery vulnerability. Using CWE to declare the problem leads to CWE-352. The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request. Impacted is integrity.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-6109. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. It demands that the victim is doing some kind of user interaction. Technical details as well as a public exploit are known.

The exploit is available 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 entries VDB-340332, VDB-352080, VDB-352081 and VDB-356524 are related to this item.

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: 4.3
VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross-site request forgery
CWE: CWE-352 / CWE-862 / CWE-863
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
04/11/2026	+0 days	VulDB entry last update

Sources

Product: github.com

Advisory: 1932
Status: Not defined

CVE: CVE-2026-6109 (🔒)
GCVE (CVE): GCVE-0-2026-6109
GCVE (VulDB): GCVE-100-356969
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/11/2026 09:54 AM
Changes: 04/11/2026 09:54 AM (58)
Complete: 🔍
Submitter: Eric-d
Cache ID: 172:B3E:179

Submit

Accepted

- Submit #791759: FoundationAgents MetaGPT 0.8.1 Cross Site Request Forgery (CWE-352) (by Eric-d)

Discussion

No comments yet. Languages: en.

Please log in to comment.