VDB-356971 · CVE-2026-6111 · ISSUE 1934

FOUNDATIONAGENTS METAGPT UP TO 0.8.1 METAGPT/UTILS/COMMON.PY DECODE_IMAGE IMG_URL_OR_B64 SERVER-SIDE REQUEST FORGERY

Summary

A vulnerability classified as critical has been found in FoundationAgents MetaGPT up to 0.8.1. Affected is the function `decode_image` of the file *metagpt/utils/common.py*. This manipulation of the argument *img_url_or_b64* causes server-side request forgery. This vulnerability is handled as CVE-2026-6111. The attack can be initiated remotely. Additionally, an exploit exists. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability has been found in FoundationAgents MetaGPT up to 0.8.1 and classified as critical. Affected by this vulnerability is the function `decode_image` of the file *metagpt/utils/common.py*. The manipulation of the argument `img_url_or_b64` with an unknown input leads to a server-side request forgery vulnerability. The CWE definition for the vulnerability is CWE-918. The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. As an impact it is known to affect confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2026-6111. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known.

It is possible to download the exploit 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-2026-21698).

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: 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: Server-side request forgery
CWE: CWE-918
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: 1934
Status: Not defined
Confirmation: 🔒

CVE: CVE-2026-6111 (🔒)
GCVE (CVE): GCVE-0-2026-6111
GCVE (VulDB): GCVE-100-356971
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013

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: 40:8F5:179

Submit

Accepted

- Submit #791762: FoundationAgents MetaGPT 0.8.1 Server-Side Request Forgery (CWE-918) (by Eric-d)

Discussion

No comments yet. Languages: en.

Please log in to comment.