COMMUNITY CONTENT

Home › Submit › 791762

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

Title FoundationAgents MetaGPT 0.8.1 Server-Side Request Forgery (CWE-918)

Description

Technical Details

A Server-Side Request Forgery (SSRF) vulnerability exists in MetaGPT due to insufficient URL validation in functions that fetch external resources, such as decode_image() in metagpt/utils/common.py and download_model().

The decode_image() function accepts an image URL or base64 string. If it starts with "http", it directly passes the URL to requests.get() without any validation of the host, IP address, or scheme. An attacker who can influence the URL parameter (e.g., via LLM prompt injection or API response manipulation) can force the server to make unauthorized HTTP requests to internal network resources or cloud metadata endpoints.

Vulnerable Code

File: metagpt/utils/common.py

Method: decode_image(img_url_or_b64)

Why: The line resp = requests.get(img_url_or_b64) performs an HTTP GET request to whatever URL is provided, lacking a blocklist for private IPs (e.g., 127.0.0.1, x.x.x.x) or an allowlist of trusted domains.

Reproduction

1. Start a local HTTP server to detect the SSRF (e.g., listening on port 18292).
2. Trigger the decode_image() function in MetaGPT and supply the internal URL http://127.0.0.1:18292/internal/admin/secret as the parameter.
3. Observe the MetaGPT process making a GET request to the local server, bypassing firewall restrictions and exposing internal network services.

Impact

- Semi-Blind SSRF: Although the response in decode_image is routed into Image.open(), filtering non-image content, attackers can still achieve network reconnaissance (port scanning), trigger state-changing actions on internal services (e.g., REST APIs), and potentially exfiltrate data via DNS or timing side channels.

Source ⚠ https://github.com/FoundationAgents/MetaGPT/issues/1934

User Eric-d (UID 96861)

Submission 03/28/2026 04:42 AM (16 days ago)

Moderation 04/11/2026 09:49 AM (14 days later)

Status Accepted

VulDB entry 358971 [FoundationAgents MetaGPT up to 0.8.1 metagpt/utils/common.py decode_image img_url_or_b64 server-side request forgery]

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling

Points 20