COMMUNITY CONTENT

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

Title	FoundationAgents MetaGPT 0.8.1 Cross Site Request Forgery (CWE-352)
Description	# Technical Details A Cross-Site Request Forgery (CSRF) vulnerability exists in the Mineflayer HTTP API of MetaGPT (metagpt/environment/minecraft/mineflayer/index.js), leading to unauthenticated Remote Code Execution (RCE). The Express.js server runs locally and exposes a /step endpoint that accepts arbitrary JavaScript code via req.body.code and executes it directly through the unsafe eval() function (evaluateCode()). This endpoint has no authentication checks and lacks CORS protection. Additionally, the server binds to x.x.x.x by default. # Vulnerable Code File: metagpt/environment/minecraft/mineflayer/index.js Method: app.post("/step", ...) & evaluateCode() Why: The server accepts POST requests containing raw JavaScript code and directly interpolates it into an eval() statement without restricting origin (CORS) or verifying the caller's identity. # Reproduction 1. Start the MetaGPT Mineflayer HTTP server locally on port 3000. 2. An attacker hosts a malicious HTML page with JavaScript that performs a blind POST request using fetch('http://127.0.0.1:3000/step', { method: 'POST', body: JSON.stringify({ code: "require('child_process').execSync('touch /tmp/csrf_rce_proof')", programs: "" }), mode: 'no-cors' }). 3. A victim running the Mineflayer server visits the attacker's page. 4. The JavaScript payload executes on the victim's machine. Verify /tmp/csrf_rce_proof exists. # Impact - Remote Code Execution (RCE): An attacker can execute arbitrary system commands, exfiltrate data, or establish a reverse shell simply by tricking the victim into opening a malicious webpage while the Mineflayer environment is running.
Source	https://github.com/FoundationAgents/MetaGPT/issues/1932
User	Eric d (UID 96861)
Submission	03/28/2026 04:36 AM (15 days ago)
Moderation	04/11/2026 09:49 AM (14 days later)
Status	Accepted

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

VulDB entry [FoundationAgents MetaGPT up to 0.8.1 Mineflayer HTTP API index.js evaluateCode cross-site request forgery]

Points 20