COMMUNITY CONTENT

Submit #782169: ScrapeGraphAI scrapegraph-ai 1.74.0 Remote Code Execution (RCE)

Title	ScrapeGraphAI scrapegraph-ai 1.74.0 Remote Code Execution (RCE)
Description	A critical Remote Code Execution vulnerability exists in the GenerateCodeNode component of ScrapeGraphAI v1.74.0. The library uses a Large Language Model (LLM) to generate Python code for data extraction from scraped web pages, then executes that code via Python's exec() built-in with a "sandbox" that exposes the full __builtins__ module, providing no actual isolation. An attacker who controls or can influence the content of a target website can embed prompt injection payloads in the HTML (e.g., within invisible HTML comments). When a victim uses ScrapeGraphAI's CodeGeneratorGraph to scrape the attacker's page, the HTML content — including the prompt injection — is fed directly into the LLM prompt. The LLM then generates Python code that may include arbitrary malicious operations (importing subprocess, executing shell commands, reading files, exfiltrating data). This code is executed via exec() with full access to Python's built-in functions, resulting in arbitrary code execution on the victim's machine.
Source	https://github.com/August829/CVEP/issues/19
User	Yu Bao (UID 88856)
Submission	03/18/2026 08:21 AM (18 days ago)
Moderation	04/04/2026 08:33 AM (17 days later)
Status	Accepted
VulDB entry	[ScrapeGraphAI scrapegraph-ai up to 1.74.0 GenerateCodeNode generate_code_node.py create_sandbox_and_execute os command injection]
Points	20

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