COMMUNITY CONTENT

Home › Submit › 784465

Submit #784465: griptape v0.19.4 Absolute Path Traversal

Title	griptape v0.19.4 Absolute Path Traversal
Description	The ComputerTool in Griptape allows agents to execute Python code by first writing the code to a file in a local working directory, which is then mounted into a container for execution. However, the filename parameter, which determines where the code is stored locally, is generated by the LLM and is not properly validated or sanitized. This lack of validation allows for a path traversal vulnerability. An attacker can use prompt injection to coerce the LLM into specifying a filename containing directory traversal sequences (e.g., ../../malicious_file). Since the file content (the code) is also controllable via prompt injection, writing to sensitive files like __init__.py or ~/.bashrc may lead to Remote Code Execution (RCE) on the host system.
Source	⚠ https://github.com/Ka7arotto/cve/blob/main/griptape/SaveCodeTool/computeTool.md
User	Goku (UID 80486)
Submission	03/21/2026 03:05 AM (16 days ago)
Moderation	04/05/2026 07:17 AM (15 days later)
Status	Accepted
VulDB entry	355391 [griptape-ai griptape 0.19.4 ComputerTool tool.py filename path traversal]
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

© 1997-2026 vuldb.com · cc by-nc-sa