COMMUNITY CONTENT

Submit #784463: griptape v0.19.4 Absolute Path Traversal

Title	griptape v0.19.4 Absolute Path Traversal
Description	The `FileManagerTool` (backed by `LocalFileManagerDriver`) in Griptape provides capabilities to list, read, and write files. However, it fails to properly sanitize file paths provided by the LLM. It directly concatenates the llm-supplied path with the working directory. This allows for a path traversal vulnerability. An attacker can use prompt injection to coerce the LLM into providing paths containing `../` sequences. This enables the agent to: 1. **Read arbitrary files** (e.g., `/etc/passwd`) via `load_files_from_disk`. 2. **List arbitrary directories** via `list_files_from_disk`. 3. **Write to arbitrary files** via `save_content_to_file` or `save_memory_artifacts_to_disk`.
Source	⚠ https://github.com/Ka7arotto/cve/blob/main/griptape/issue_fileManagerTool/issue.md
User	Goku (UID 80486)
Submission	03/21/2026 02:57 AM (16 days ago)
Moderation	04/05/2026 07:17 AM (15 days later)
Status	Accepted
VulDB entry	355389 [griptape-ai griptape 0.19.4 FileManagerTool 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