VDB-355389 · CVE-2026-5595 · GCVE-100-355389

# GRIPTAPE-AI GRIPTAPE 0.19.4 FILEMANAGERTOOL PATH TRAVERSAL

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
|---|---|---|
| 5.7 | $0-$5k | 2.45- |

## Summary

A vulnerability classified as critical has been found in griptape-ai griptape 0.19.4. Affected by this issue is the function `load_files_from_disk/list_files_from_disk/save_content_to_file/save_memory_artifacts_to_disk` of the component *FileManagerTool*. Performing a manipulation results in path traversal. This vulnerability is cataloged as CVE-2026-5595. It is possible to initiate the attack remotely. Furthermore, there is an exploit available. The vendor was contacted early about this disclosure but did not respond in any way.

## Details

A vulnerability was found in griptape-ai griptape 0.19.4. It has been classified as critical. This affects the function `load_files_from_disk/list_files_from_disk/save_content_to_file/save_memory_artifacts_to_disk` of the component *FileManagerTool*. The manipulation with an unknown input leads to a path traversal vulnerability. CWE is classifying the issue as CWE-22. The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared at github.com. This vulnerability is uniquely identified as CVE-2026-5595. The exploitability is told to be easy. It is possible to initiate the attack remotely. Technical details and a public exploit are known. MITRE ATT&CK project uses the attack technique T1006 for this issue.

The exploit is shared for download at github.com. It is declared as proof-of-concept. The vendor was contacted early about this disclosure but did not respond in any way.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

The entries VDB-355390 and VDB-355391 are related to this item.

## Product

**Type**

- Artificial Intelligence Software

**Vendor**

- griptape-ai

**Name**

- griptape

**Version**

- 0.19.4

## CPE 2.3

- 🔒

## CPE 2.2

- 🔒

## CVSSv4

**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv3

**VulDB Meta Base Score**: 6.3
**VulDB Meta Temp Score**: 5.7

**VulDB Base Score**: 6.3
**VulDB Temp Score**: 5.7
**VulDB Vector**: 🔒
**VulDB Reliability**: 🔍

## CVSSv2

**VulDB Base Score**: 🔒
**VulDB Temp Score**: 🔒
**VulDB Reliability**: 🔍

## Exploiting

**Class**: Path traversal
**CWE**: CWE-22
**CAPEC**: 🔒
**ATT&CK**: 🔒

**Physical**: No
**Local**: No
**Remote**: Yes

**Availability**: 🔒
**Access**: Public
**Status**: Proof-of-Concept
**Download**: 🔒
**Price Prediction**: 🔍
**Current Price Estimation**: 🔒

## Threat Intelligence

**Interest**: 🔍
**Active Actors**: 🔍
**Active APT Groups**: 🔍

## Countermeasures

**Recommended**: no mitigation known
**Status**: 🔍

**0-Day Time**: 🔒

## Timeline

| | | |
|---|---|---|
| **04/05/2026** | | Advisory disclosed |
| **04/05/2026** | +0 days | VulDB entry created |
| **04/05/2026** | +0 days | VulDB entry last update |

## Sources

**Advisory**: github.com
**Status**: Not defined

**CVE**: CVE-2026-5595 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5595
**GCVE (VulDB)**: GCVE-100-355389
**scip Labs**: https://www.scip.ch/en/?labs.20161013
**See also**: 🔒

## Entry

**Created**: 04/05/2026 07:22 AM
**Changes**: 04/05/2026 07:22 AM (57)
**Complete**: 🔍
**Submitter**: Goku
**Cache ID**: 9:E28:179

## Submit

**Accepted**

- Submit #784463: griptape v0.19.4 Absolute Path Traversal (by Goku)

## Discussion

No comments yet. Languages: en.

Please log in to comment.