VDB-355391 · CVE-2026-5597 · GCVE-100-355391

# GRIPTAPE-AI GRIPTAPE 0.19.4 COMPUTERTOOL TOOL.PY FILENAME PATH TRAVERSAL

| CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score |
|---|---|---|
| 5.7 | $0-$5k | 2.87- |

## Summary

A vulnerability, which was classified as critical, has been found in griptape-ai griptape 0.19.4. This vulnerability affects unknown code of the file *griptape\tools\computer\tool.py* of the component *ComputerTool*. The manipulation of the argument *filename* leads to path traversal. This vulnerability is documented as CVE-2026-5597. The attack can be initiated remotely. Additionally, an exploit exists. 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 rated as critical. This issue affects an unknown functionality of the file *griptape\tools\computer\tool.py* of the component *ComputerTool*. The manipulation of the argument `filename` with an unknown input leads to a path traversal vulnerability. Using CWE to declare the problem leads to 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. Impacted is confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-5597. The exploitation is known to be easy. The attack may be initiated remotely. Technical details as well as a public exploit are known. The attack technique deployed by this issue is T1006 according to MITRE ATT&CK.

The exploit is available 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.

Entries connected to this vulnerability are available at VDB-351162, VDB-351930, VDB-352589 and VDB-353784.

## 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-2026-5597 (🔒)
**GCVE (CVE)**: GCVE-0-2026-5597
**GCVE (VulDB)**: GCVE-100-355391
**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 (58)
**Complete**: 🔍
**Submitter**: Goku
**Cache ID**: 172:341:179

## Submit

**Accepted**

- Submit #784465: griptape v0.19.4 Absolute Path Traversal (by Goku)

## Discussion

No comments yet. Languages: en.

Please log in to comment.