VDB-355383 · CVE-2026-5584 · GCVE-100-355383

FOSOWL AGENTICSEEK 0.1.0 QUERY ENDPOINT PYINTERPRETER.PY PYINTERPRETER.EXECUTE CODE INJECTION

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
6.6	$0-$5k	4.61-

Summary

A vulnerability was found in Fosowl agenticSeek 0.1.0. It has been rated as critical. The affected element is the function `PyInterpreter.execute` of the file *sources/tools/PyInterpreter.py* of the component *query Endpoint*. Performing a manipulation results in code injection. This vulnerability was named CVE-2026-5584. The attack may be initiated remotely. In addition, an exploit is available. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability classified as critical has been found in Fosowl agenticSeek 0.1.0. This affects the function `PyInterpreter.execute` of the file *sources/tools/PyInterpreter.py* of the component *query Endpoint*. The manipulation with an unknown input leads to a code injection vulnerability. CWE is classifying the issue as CWE-94. The product constructs all or part of a code segment using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the syntax or behavior of the intended code segment. This is going to have an impact on confidentiality, integrity, and availability.

It is possible to read the advisory at github.com. This vulnerability is uniquely identified as CVE-2026-5584. The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. Technical details and a public exploit are known. The attack technique deployed by this issue is T1059 according to MITRE ATT&CK.

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.

See VDB-337789 for similar entry.

Product

Vendor

- Fosowl

Name

- agenticSeek

Version

- 0.1.0

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 6.6

VulDB Base Score: 7.3
VulDB Temp Score: 6.6
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Code injection
CWE: CWE-94 / CWE-74 / CWE-707
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

04/04/2026		Advisory disclosed
04/04/2026	+0 days	VulDB entry created
04/04/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2026-5584 (🔒)
GCVE (CVE): GCVE-0-2026-5584
GCVE (VulDB): GCVE-100-355383
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/04/2026 11:36 PM
Changes: 04/04/2026 11:36 PM (57)
Complete: 🔍
Submitter: Yu Bao
Cache ID: 135:BE2:179

Submit

Accepted

- Submit #784052: Fosowl agenticSeek 0.1.0 Remote Code Execution (by Yu Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.