VDB-355415 · CVE-2026-5625 · ISSUE 1692

ASSAFELOVIC GPT-RESEARCHER UP TO 3.4.3 WEBSOCKET INTERFACE RESEARCHER.PY TASK CROSS SITE SCRIPTING

CVSS Meta Temp Score	Current Exploit Price (≈)	CTI Interest Score
3.9	$0-$5k	2.52-

Summary

A vulnerability marked as problematic has been reported in assafelovic gpt-researcher up to 3.4.3. Impacted is an unknown function of the file *gpt_researcher/skills/researcher.py* of the component *WebSocket Interface*. The manipulation of the argument *task* leads to cross site scripting. This vulnerability is referenced as CVE-2026-5625. Remote exploitation of the attack is possible. Furthermore, an exploit is available. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability was found in assafelovic gpt-researcher up to 3.4.3 and classified as problematic. This issue affects an unknown code of the file *gpt_researcher/skills/researcher.py* of the component *WebSocket Interface*. The manipulation of the argument `task` with an unknown input leads to a cross site scripting vulnerability. Using CWE to declare the problem leads to CWE-79. The product does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users. Impacted is integrity.

It is possible to read the advisory at github.com. The identification of this vulnerability is CVE-2026-5625. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. It demands that the victim is doing some kind of user interaction. Technical details as well as a public exploit are known. The attack technique deployed by this issue is T1059.007 according to MITRE ATT&CK.

The exploit is available at github.com. It is declared as proof-of-concept. The project was informed of the problem early through an issue report but has not responded yet.

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

Similar entry is available at VDB-314089.

Product

Type

- Artificial Intelligence Software

Vendor

- assafelovic

Name

- gpt-researcher

Version

- 3.4.0
- 3.4.1
- 3.4.2
- 3.4.3

Website

- Product: https://github.com/assafelovic/gpt-researcher/

CPE 2.3

- 🔒
- 🔒
- 🔒

CPE 2.2

- 🔒
- 🔒
- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 4.3
VulDB Meta Temp Score: 3.9

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Cross site scripting
CWE: CWE-79 / CWE-94 / CWE-74
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

Product: github.com

Advisory: 1692
Status: Not defined

CVE: CVE-2026-5625 (🔒)
GCVE (CVE): GCVE-0-2026-5625
GCVE (VulDB): GCVE-100-355415
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 07:01 PM
Changes: 04/05/2026 07:01 PM (59)
Complete: 🔍
Submitter: Yu_Bao
Cache ID: 135:6B5:179

Submit

Accepted

- Submit #785832: assafelovic gpt-researcher 3.4.3 Reflected Cross-Site Scripting (XSS) (by Yu_Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.

© 1997-2026 vuldb.com · cc by-nc-sa

v20.2.0