VDB-355418 · CVE-2026-5630 · ISSUE 1693

ASSAFELOVIC GPT-RESEARCHER UP TO 3.4.3 REPORT API BACKEND/SERVER/APP.PY CROSS SITE SCRIPTING

CVSS Meta Temp Score | Current Exploit Price (≈) | CTI Interest Score

3.9 | $0-$5k | 2.18

Summary

A vulnerability classified as problematic was found in assafelovic gpt-researcher up to 3.4.3. This affects an unknown function of the file *backend/server/app.py* of the component *Report API*. Such manipulation leads to cross site scripting. This vulnerability is listed as CVE-2026-5630. The attack may be performed from remote. In addition, 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. It has been rated as problematic. Affected by this issue is an unknown function of the file *backend/server/app.py* of the component *Report API*. The manipulation 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.

The advisory is available at github.com. This vulnerability is handled as CVE-2026-5630. The exploitation is known to be easy. The attack may be launched remotely. No form of authentication is required for exploitation. Successful exploitation requires user interaction by the victim. Technical details as well as a public exploit are known. This vulnerability is assigned to T1059.007 by the MITRE ATT&CK project.

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.

See VDB-81538 for similar entry.

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: 1693
Status: Not defined

CVE: CVE-2026-5630 (🔒)
GCVE (CVE): GCVE-0-2026-5630
GCVE (VulDB): GCVE-100-355418
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 09:17 PM
Changes: 04/05/2026 09:17 PM (58)
Complete: 🔍
Submitter: Yu-Bao
Cache ID: 172:CFF:179

Submit

Accepted

- Submit #785856: assafelovic gpt-researcher 3.4.3 Stored Cross-Site Scripting (XSS) (by Yu-Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.