VDB-355421 · CVE-2026-5633 · ISSUE 1696

ASSAFELOVIC GPT-RESEARCHER UP TO 3.4.3 WS ENDPOINT SOURCE_URLS SERVER-SIDE REQUEST FORGERY

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

6.6 | $0-$5k | 2.95

Summary

A vulnerability has been found in assafelovic gpt-researcher up to 3.4.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the component *ws Endpoint*. The manipulation of the argument *source_urls* leads to server-side request forgery. This vulnerability is documented as CVE-2026-5633. The attack can be initiated remotely. Additionally, an exploit exists. The project was informed of the problem early through an issue report but has not responded yet.

Details

A vulnerability, which was classified as critical, has been found in assafelovic gpt-researcher up to 3.4.3. This issue affects an unknown part of the component *ws Endpoint*. The manipulation of the argument `source_urls` with an unknown input leads to a server-side request forgery vulnerability. Using CWE to declare the problem leads to CWE-918. The web server receives a URL or similar request from an upstream component and retrieves the contents of this URL, but it does not sufficiently ensure that the request is being sent to the expected destination. Impacted is confidentiality, integrity, and availability.

The advisory is shared at github.com. The identification of this vulnerability is CVE-2026-5633. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details as well as a public exploit are known.

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.

The vulnerability is also documented in the vulnerability database at EUVD (EUVD-2026-19190). Entry connected to this vulnerability is available at VDB-355419.

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: 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: Server-side request forgery
CWE: CWE-918
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
04/06/2026	+1 days	VulDB entry last update

Sources

Product: github.com

Advisory: 1696
Status: Not defined

CVE: CVE-2026-5633 (🔒)
GCVE (CVE): GCVE-0-2026-5633
GCVE (VulDB): GCVE-100-355421
EUVD: 🔒
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 04/05/2026 09:18 PM
Updated: 04/06/2026 11:02 AM
Changes: 04/05/2026 09:18 PM (58), 04/06/2026 11:02 AM (1)
Complete: 🔍
Submitter: Yu-Bao
Cache ID: 64:401:179

Submit

Accepted

- Submit #785876: assafelovic gpt-researcher 3.4.3 Unauthenticated Server-Side Request Forgery (SSRF) (by Yu-Bao)

Discussion

No comments yet. Languages: en.

Please log in to comment.