



VDB-354653 · CVE-2026-5321 · GCVE-100-354653

VANNA-AI VANNA UP TO 2.0.2 FASTAPI/FLASK SERVER CROSS-DOMAIN POLICY

CVSS Meta Temp Score 

3.9

Current Exploit Price (≈) 

\$0-\$5k

CTI Interest Score 

1.20-

Summary

A vulnerability was found in [vanna-ai vanna up to 2.0.2](#). It has been classified as [critical](#). This affects an unknown part of the component *FastAPI/Flask Server*. The manipulation leads to cross-domain policy. This vulnerability is listed as [CVE-2026-5321](#). 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 was found in [vanna-ai vanna up to 2.0.2](#). It has been rated as problematic. This issue affects an unknown code block of the component *FastAPI/Flask Server*. The manipulation with an unknown input leads to a cross-domain policy vulnerability. Using CWE to declare the problem leads to [CWE-942](#). The product uses a cross-domain policy file that includes domains that should not be trusted. Impacted is integrity.

The advisory is shared at [github.com](#). The identification of this vulnerability is [CVE-2026-5321](#). The exploitation is known to be easy. The attack may be initiated remotely. Technical details are unknown but a public exploit is available.

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.

See [VDB-300237](#), [VDB-300385](#), [VDB-300429](#) and [VDB-300487](#) for similar entries.

Product

Type

- [Artificial Intelligence Software](#)

Vendor

- [vanna-ai](#)




Name

- [vanna](#)



Version

- [2.0.0](#)
- [2.0.1](#)
- [2.0.2](#)

CPE 2.3

- 
- 
- 

CPE 2.2

- 
- 
- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CVSSv3

VulDB Meta Base Score: 4.3

VulDB Meta Temp Score: 3.9

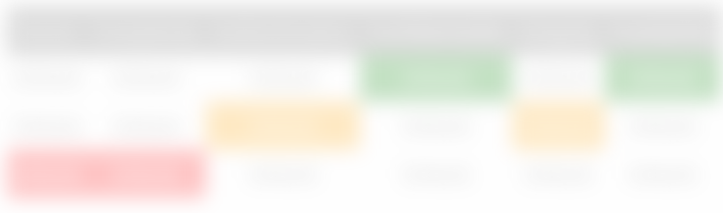
VulDB Base Score: 4.3

VulDB Temp Score: 3.9

VulDB Vector: 

VulDB Reliability: 

CVSSv2



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

Exploiting

Class: Cross-domain policy
CWE: [CWE-942](#) / [CWE-346](#) / [CWE-345](#)
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

04/01/2026		Advisory disclosed
04/01/2026	+0 days	VulDB entry created
04/01/2026	+0 days	VulDB entry last update

Sources

Advisory: github.com

Status: Not defined

CVE: [CVE-2026-5321](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5321](#)

GCVE (VulDB): [GCVE-100-354653](#)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 🔒

Entry

Created: 04/01/2026 03:05 PM

Changes: 04/01/2026 03:05 PM (56)

Complete: 🔍

Submitter: [Yu_Bao](#)

Cache ID: 172:301:179

Submit

Accepted

- [Submit #780729](#): vanna-ai vanna 2.0.2 CORS Origin Reflection with Credentials (by Yu_Bao)

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)

