



VDB-355071 · CVE-2026-5467 · GCVE-100-355071

CASDOOR 2.356.0 OAUTH AUTHORIZATION REQUEST REDIRECT_URI

CVSS Meta Temp Score ⓘ

3.9

Current Exploit Price (≈) ⓘ

\$0-\$5k

CTI Interest Score ⓘ

1.54

Summary

A vulnerability has been found in [Casdoor 2.356.0](#) and classified as [problematic](#). This affects an unknown part of the component *OAuth Authorization Request Handler*. Performing a manipulation of the argument *redirect_uri* results in redirect. This vulnerability is identified as [CVE-2026-5467](#). The attack can be initiated remotely. Additionally, an exploit exists. The vendor was contacted early about this disclosure but did not respond in any way.

Details

A vulnerability, which was classified as [problematic](#), was found in [Casdoor 2.356.0](#). This affects an unknown part of the component *OAuth Authorization Request Handler*. The manipulation of the argument *redirect_uri* with an unknown input leads to a redirect vulnerability. CWE is classifying the issue as [CWE-601](#). A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks. This is going to have an impact on integrity.

This vulnerability is uniquely identified as [CVE-2026-5467](#). The exploitability is told to be easy. It is possible to initiate the attack remotely. No form of authentication is needed for exploitation. It demands that the victim is doing some kind of user interaction. Technical details and a public exploit are known. The attack technique deployed by this issue is [T1204.001](#) according to MITRE ATT&CK.

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.

Entries connected to this vulnerability are available at [VDB-247965](#), [VDB-250756](#), [VDB-284521](#) and [VDB-285702](#).

Product

Name

- [Casdoor](#)

Version

- [2.356.0](#)

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: Redirect

CWE: [CWE-601](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🔒

Timeline

- 04/03/2026 | Advisory disclosed
- 04/03/2026 | +0 days | VulDB entry created
- 04/03/2026 | +0 days | VulDB entry last update

Sources

Status: Not defined

CVE: [CVE-2026-5467](#) (🔒)

GCVE (CVE): [GCVE-0-2026-5467](#)

GCVE (VuIDB): [GCVE-100-355071](#)

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

See also: 🔒

Entry

Created: 04/03/2026 09:31 AM

Changes: 04/03/2026 09:31 AM (53)

Complete: 🔍

Submitter: [Ghufran Khan](#)

Cache ID: 74:E9C:179

Submit

Accepted

- [Submit #781769](#): Casdoor v2.356.0 Open Redirect (by [Ghufran Khan](#))

Discussion

No comments yet. Languages: en.

[Please log in to comment.](#)