VDB-307180 · CVE-2025-4210 · GCVE-100-307180

CASDOOR UP TO 1.811.0 SCIM USER CREATION ENDPOINT CONTROLLERS/SCIM.GO HANDLESCIM AUTHORIZATION

A vulnerability classified as critical was found in Casdoor up to 1.811.0. This vulnerability affects the function `HandleScim` of the file *controllers/scim.go* of the component *SCIM User Creation Endpoint*. The manipulation with an unknown input leads to a authorization vulnerability. The CWE definition for the vulnerability is CWE-639. The system's authorization functionality does not prevent one user from gaining access to another user's data or record by modifying the key value identifying the data. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at github.com. This vulnerability was named CVE-2025-4210. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details and also a exploit are known.

It is declared as highly functional.

Upgrading to version 1.812.0 eliminates this vulnerability. The upgrade is hosted for download at github.com. Applying the patch 3d12ac8dc2282369296c3386815c00a06c6a92fe is able to eliminate this problem. The bugfix is ready for download at github.com. The best possible mitigation is suggested to be upgrading to the latest version.

Similar entries are available at VDB-191997, VDB-208210, VDB-215065 and VDB-232149.

Product

Name

- Casdoor

Version

- 1.811

License

- open-source

CPE 2.3

- 🔒

CPE 2.2

- 🔒

CVSSv4

VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv3

VulDB Meta Base Score: 7.3
VulDB Meta Temp Score: 7.0

VulDB Base Score: 7.3
VulDB Temp Score: 7.0
VulDB Vector: 🔒
VulDB Reliability: 🔍

CVSSv2

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

Exploiting

Class: Authorization
CWE: CWE-639 / CWE-285 / CWE-266
CAPEC: 🔒
ATT&CK: 🔒

Local: No
Remote: Yes

Availability: 🔒
Status: Highly functional

Price Prediction: 🔍
Current Price Estimation: 🔒

[redacted]

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade
Status: 🔍

0-Day Time: 🔒

Upgrade: Casdoor 1.812.0
Patch: 3d12ac8dc2282369296c3386815c00a06c6a92fe

Timeline

05/02/2025		Advisory disclosed
05/02/2025	+0 days	VulDB entry created
05/02/2025	+0 days	VulDB entry last update

Sources

Advisory: 3d12ac8dc2282369296c3386815c00a06c6a92fe
Status: Confirmed

CVE: CVE-2025-4210 (🔒)
GCVE (CVE): GCVE-0-2025-4210
GCVE (VulDB): GCVE-100-307180
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/02/2025 12:50 PM
Changes: 05/02/2025 12:50 PM (57), 05/02/2025 12:51 PM (3)
Complete: 🔍
Submitter: krav
Cache ID: 5:9DD:101

Submit

Accepted

- Submit #556201: Casbin Casdoor v1.430.0-v1.812.0 Authorization Bypass (by krav)

Discussion

No comments yet. Languages: en.

Please log in to comment.