Submit #556201: Casbin Casdoor v1.430.0-v1.812.0 Authorization Bypass

Title	Casbin Casdoor v1.430.0-v1.812.0 Authorization Bypass
Description	All versions of this IAM product released between Oct 2023 and Jan 2025 are vulnerable to a remote attacker creating an admin account without authenticating. The endpoint to create SCIM users is simply lacking authentication middleware, creating a SCIM user will associate a corresponding local user. To use the exploit, issue a POST request to `/scim/Users`: ``` {"active":true,"displayName":"Admin","emails":[{"value":"cool@email.com"}],"password":"cool-password"} ``` The developers silently issued a fix: https://github.com/casdoor/casdoor/commit/3d12ac8dc2282369296c3386815c00a06c6a92fe Developers have not responded to email, on Discord they responded by kicking me. This is being actively exploited in the wild.
User	krav (UID 84007)
Submission	04/11/2025 12:13 AM (23 days ago)
Moderation	05/02/2025 12:45 PM (22 days later)
Status	Accepted
VulDB Entry	307180 [Casdoor up to 1.811.0 SCIM User Creation Endpoint controllers/scim.go HandleScim authorization]
Points	17

Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling