CVE-2026-30269 – Improper Access Control in Doorman Allows Privilege Escalation

2026-04-19

目录

CVE-2026-30269: Improper Access Control in Doorman Allows Privilege Escalation

Summary

Doorman `v0.1.0` and `v1.0.2` allow an authenticated user to update their own account and change `role` via `PUT /platform/user/{username}` without requiring `manage_users` permission in the self-update path.

This can let a low-privileged user promote themselves to a stronger non-admin role.

- **CVE:** CVE-2026-30269
- **Type:** Improper Access Control
- **Impact:** Privilege Escalation
- **Attack Vector:** Remote authenticated request

Affected Product

- **Vendor:** Doorman Dev, LLC
- **Repository:** https://github.com/apidoorman/doorman
- **Affected versions:** `v0.1.0`, `v1.0.2`

Root Cause

- `backend-services/routes/user_routes.py:update_user` allows self-update without `manage_users`
- `backend-services/models/update_user_model.py` accepts `role`
- `backend-services/services/user_service.py:update_user` persists non-null fields directly

Minimal PoC

Fix Commit

The upstream project added field-level authorization in:

- **Commit:** `0c8791cca8501bb6be45b172db934ac72ac03c84`
- **Link:** https://github.com/apidoorman/doorman/commit/0c8791cca8501bb6be45b172db934ac72ac03c84

This commit blocks restricted fields (`role` , `groups` , `active` , `username`) during self-update when the caller does not have `manage_users` .

Credits

Discovered by **orxiain**.

#CVE #Doorman #Privilege Escalation