security(kobo_auth): close IDOR in token generation / deletion (#1303 upstream) #18

Merged **new-usemame** merged 1 commit into `main` from `security/kobo-auth-idor-1303`

2 days ago

new-usemame commented 2 days ago — Owner

Severity: HIGH

Closes the IDOR vulnerability described in upstream issue #1303. Upstream has no fix PR at time of writing.

Bug

`cps/kobo_auth.py` exposed two routes:

- `GET /kobo_auth/generate_auth_token/int:user_id`
- `POST /kobo_auth/deleteauthtoken/int:user_id`

Both were gated **only** by `@user_login_required`. Neither verified that `user_id` matched `current_user.id` or that the requester was admin.

Effect:

- Any authenticated user could request a Kobo auth token for *any* other user_id and walk away with their token — full Kobo-sync impersonation.
- Any authenticated user could revoke any other user's token — soft DoS / lockout.

Fix

Add an IDOR guard at the top of both view functions:

```python
if current_user.id != user_id and not current_user.role_admin():
abort(403)
```

Same pattern `cps/admin.py` uses for admin-only routes. `current_user` and `abort` are already imported in this file. The guard short-circuits unauthorized access before any DB query runs.

Risk

Defensive. The intended use case is the user setting up their own Kobo, which still works — `current_user.id == user_id`. Admin can still mint/delete tokens for any user (e.g., to help a household member). Non-self / non-admin requests now return 403 instead of leaking a token.

Test plan

- [ ] Maggie can still set up her own Kobo at `/kobo_auth/generate_auth_token/<her_user_id>` (passes the guard).
- [ ] Admin can mint a token on behalf of another user (passes `role_admin()`).
- [ ] Non-admin requesting another user's id returns 403 (was: returns leaked token).
- [ ] Existing CI: `Test Suite / Fast Tests` green.
- [ ] `validate-author` green.

Why we're shipping ahead of upstream

Upstream issue is open with no comments and no fix PR. Our deployment runs Kobo sync. This is a 12-line single-file change that mirrors an existing in-repo pattern; landing it locally has higher value than waiting for an upstream merge.

Manual recovery

If the operator wants to roll back: `gh pr revert` on the merged commit, or hand-revert `cps/kobo_auth.py` lines 70-78 and 112-122.

`fix(kobo_auth): close IDOR in generate_auth_token / delete_auth_token…` ··· ✓ `93c82dc`

new-usemame added the needs-review label 2 days ago

new-usemame mentioned this pull request 2 days ago

security(cover_enforcer): replace os.system shell-interpolation with shutil #20

Merged

3 tasks

new-usemame merged commit `9f50bb2` into `main` 2 days ago

10 checks passed

View details

new-usemame deleted the `security/kobo-auth-idor-1303` branch 2 days ago

new-usemame added a commit that referenced this pull request 2 days ago

`security(cover_enforcer): replace os.system shell-interpolation with …` ··· `b70fb53`

Reviewers

No reviews

Assignees

No one assigned

Labels

needs-review

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

1 participant