New issue

IDOR in Kobo Auth Token Generation Enables Account Impersonation #1303

Open

menelausx opened last week

The Kobo authentication flow contains an insecure direct object reference (IDOR) vulnerability in the /kobo_auth/generate_auth_token/int:user_id endpoint. The route is protected only by @user_login_required but does not verify that the requested user_id matches the current user or that the requester has admin privileges.

As a result, any authenticated user can generate or retrieve a Kobo authentication token for arbitrary users by supplying their user_id. The token is then returned in the response, exposing sensitive authentication credentials.

new-usemame mentioned this 2 days ago

security(kobo_auth): close IDOR in token generation / deletion (#1303 upstream) new-usemame/Calibre-Web-NextGen#18

new-usemame added a commit that references this issue 2 days ago

`fix(kobo_auth): close IDOR in generate_auth_token / delete_auth_token.` ···

Verified `9f50bb2`

new-usemame 7 hours ago

Patched in Calibre-Web-NextGen v4.0.7 at `9f50bb2` : `/kobo_auth/generate_auth_token` and `/deleteauthtoken` now reject when `current_user.id != user_id` and not admin. No upstream PR existed; fix written for the fork (12 LOC, mirrors `cps/admin.py @admin_required` pattern), mergeable back if upstream resumes.

Drop-in image: `ghcr.io/new-usemame/calibre-web-nextgen:latest` (community-maintained CWA build).
Tracker: https://github.com/new-usemame/Calibre-Web-NextGen/issues.

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants