New issue

Redesign EditSelf permission: proper self-service portal #8617

Closed

Labels Security enhancement

Milestone 7.2.0

DawoudIO opened last week Contributor

Context

The `EditSelf` permission flag allows users to edit their own record and family members. However, the current implementation has issues:

1. **IDOR vulnerability (GHSA-5w59-32c8-933v)**: The API doesn't enforce EditSelf scoping — any authenticated user can read any person via `GET /api/person/{id}`
2. **No self-service UI**: There's no dedicated UI for EditSelf users — they get the full admin interface but most features return 403
3. **Permission naming confusion**: `canEditPerson()` is used as both an edit AND view gate

Current State

- `EditSelf=1` with all other permissions at 0 creates a user who can log in but has no meaningful UI
- The legacy `PersonView.php` checks `canEditPerson()` but the API layer didn't (now temporarily fixed)
- PR security: block no-permission users + fix IDOR on person API #8616 blocks EditSelf-only users and redirects to family verify page as an interim measure

Proposed Redesign

1. **Create a self-service portal** at `/self-service/` or `/my-family/` that EditSelf users see after login
2. **Portal features**: View/edit own profile, view/edit family members, family verify flow

3. **Separate view vs edit permissions**: Consider `ViewRecords` permission distinct from `EditRecords`
4. **API scoping**: API routes should respect EditSelf scoping consistently

Interim Fix (PR #8616)

EditSelf-only users are redirected to the family verify page (if they have a family) or shown a "limited access" message. This prevents the IDOR while the full redesign is planned.

Related

- GHSA-5w59-32c8-933v (IDOR on person API)
- PR security: add auth middleware to person API routes #8611 (reverted — too restrictive)
- PR security: block no-permission users + fix IDOR on person API #8616 (interim block + redirect)

DawoudIO added this to the 7.2.0 milestone last week

DawoudIO added enhancement Security last week

DawoudIO added a commit that references this issue last week

`security: block EditSelf-only users + add canEditPerson IDOR check` … `37c0360`

DawoudIO mentioned this last week

security: block no-permission users + fix IDOR on person API #8616

DawoudIO added a commit that references this issue last week

`security: add /external/limited-access page for no-permission users` … `18b1efe`

DawoudIO mentioned this last week

User limited only to self editing #237

DawoudIO 5 days ago Contributor Author •••

Closing — the immediate problem (no-permission users could access the full admin UI) is fully resolved by:

- **PR security: block no-permission users + fix IDOR on person API #8616** — blocks users with no admin permissions, redirects them to `/external/limited-access`
- **PR fix: improve family verify page UX — replace broken FAB, add navigation #8620** — fixes the family verify page UX (broken FAB, missing logout)

The limited-access page provides a "Verify Family Info" link and a "Log Out" button, which covers the practical use case. A dedicated self-service portal can be a separate feature request if needed.

DawoudIO closed this as completed 5 days ago

Metadata

Assignees

No one assigned

Labels

Security enhancement

Type

No type

Projects

No projects

Milestone

7.2.0
Closed 2 days ago, 99% complete

Relationships

None yet

Development

No branches or pull requests

Participants