enchant97 / **note-mark** Public

Code | Issues 9 | Pull requests | Discussions | Actions | Projects | Se

Commit 6593898

enchant97 committed 5 days ago Verified

```
(backend) prevent CWE-862 for asset access

this is a very unlikely attack, due to needing to know the exact UUID.
However, it's now fixed!

fixes GHSA-p5w6-75f9-cc2p
```

main · v0.19.2

1 parent 6bb6284 commit 6593898

2 files changed +20 -2 lines changed

Top

Filter files…

- backend
  - handlers
    - assets.go
  - services
    - assets.go

2 files changed +20 -2 lines changed

Search within code

backend/handlers/assets.go

```
@@ -122,11 +122,13 @@ func (h AssetsHandler) GetNoteAssets(
122 122         }
123 123     }
124 124
125         - // TODO Work out way to authenticate this
126 125     func (h AssetsHandler) GetNoteAssetContentByID(
127 126         ctx context.Context,
```

```
128  127        input *GetNoteAssetContentByIDInput) (*huma.StreamResponse, error) {
     128  +     authDetails, _ := h.AuthProvider.TryGetAuthDetails(ctx)
     129  +     optionalUserUID := authDetails.GetOptionalUserID()
129  130        if asset, info, stream, err := h.AssetsService.GetNoteAssetContentByID(
     131  +         optionalUserUID,
130  132            input.NoteID,
131  133            input.AssetID,
132  134            h.Storage); err != nil {
```

backend/services/assets.go

```
     @@ -2,6 +2,7 @@ package services
2    2
3    3    import (
4    4        "io"
     5  +     "log"
5    6
6    7        "github.com/enchant97/note-mark/backend/db"
7    8        "github.com/enchant97/note-mark/backend/storage"
     @@ -94,11 +95,26 @@ func (s AssetsService) GetNoteAssets(
94   95   }
95   96
96   97   func (s AssetsService) GetNoteAssetContentByID(
     98  +     currentUserID *uuid.UUID,
97   99        noteID uuid.UUID,
98   100       assetID uuid.UUID,
99   101       storage_backend storage.StorageController) (db.NoteAsset,
     storage.AssetFileInfo, io.ReadCloser, error) {
     102 +     // check whether can get note asset
     103 +     var noteExists int64
     104 +     if err := db.DB.
     105 +         Model(&db.Note{}).
     106 +         Preload("Book").
     107 +         Joins("JOIN books ON books.id = notes.book_id").
     108 +         Where("owner_id = ? OR is_public = ?", currentUserID, true).
     109 +         Where("notes.id = ?", noteID).
     110 +         Count(&noteExists).Error; err != nil {
     111 +         log.Println(err)
```

```
        112 +         return db.NoteAsset{}, storage.AssetFileInfo{}, nil,
            dbErrorToServiceError(err)
        113 +     } else if noteExists == 0 {
        114 +         return db.NoteAsset{}, storage.AssetFileInfo{}, nil, NotFoundError
        115 +     }
        116 +     // get note asset
100     117       var noteAsset db.NoteAsset
101             -
102     118       if err := db.DB.
103     119           First(&noteAsset, "id = ? AND note_id = ?", assetID, noteID).
104     120           Error; err != nil {
```

Comments 0

Please sign in to comment.