leepeuker / **movary** Public

Code Issues 71 Pull requests 18 Discussions Actions Security and

Commit 92c7400

leepeuker authored last week · ✓ 1 / 1 · Verified

```
Merge pull request #749 from leepeuker/privilege-escalation-GHSA-7r3f-9fwv-p43w

Fixed privilege escalation in user management
```

main (#749) · 0.71.1

2 parents a0d96a9 + 21cd4c4 commit 92c7400

2 files changed +10 -4 lines changed

Top

Filter files…

- settings
  - routes.php
- src/HttpController/Web
  - UserController.php

2 files changed +10 -4 lines changed

Search within code

settings/routes.php

```
@@ -146,8 +146,14 @@ function addWebRoutes(RouterService $routerService,
FastRoute\RouteCollector $ro
146  146      $routes->add('POST', '/settings/netflix/import',
[Web\NetflixController::class, 'importNetflixData'],
[Web\Middleware\UserIsAuthenticated::class]);
147  147      $routes->add('GET', '/settings/integrations/mastodon',
[Web\SettingsController::class, 'renderMastodonPage'],
[Web\Middleware\UserIsAuthenticated::class]);
148  148      $routes->add('POST', '/settings/integrations/mastodon',
[Web\SettingsController::class, 'updateMastodon'],
```

```
                [Web\Middleware\UserIsAuthenticated::class]);
149         -     $routes->add('GET', '/settings/users', [Web\UserController::class,
                'fetchUsers']);
150         -     $routes->add('POST', '/settings/users', [Web\UserController::class,
                'createUser']);
        149 +     $routes->add('GET', '/settings/users', [Web\UserController::class,
                'fetchUsers'], [
        150 +         Web\Middleware\UserIsAuthenticated::class,
        151 +         Web\Middleware\UserIsAdmin::class
        152 +     ]);
        153 +     $routes->add('POST', '/settings/users', [Web\UserController::class,
                'createUser'], [
        154 +         Web\Middleware\UserIsAuthenticated::class,
        155 +         Web\Middleware\UserIsAdmin::class
        156 +     ]);
151     157         $routes->add('PUT', '/settings/users/{userId:\d+}',
                [Web\UserController::class, 'updateUser'],
                [Web\Middleware\UserIsAuthenticated::class]);
152     158         $routes->add('DELETE', '/settings/users/{userId:\d+}',
                [Web\UserController::class, 'deleteUser'],
                [Web\Middleware\UserIsAuthenticated::class]);
153     159         $routes->add('GET', '/settings/locations', [Web\LocationController::class,
                'fetchLocations'], [Web\Middleware\UserIsAuthenticated::class]);
```

src/HttpController/Web/UserController.php

```
                @@ -23,7 +23,7 @@ public function __construct(
23      23          public function createUser(Request $request) : Response
24      24          {
25      25              if ($this->authenticationService->isUserAuthenticatedWithCookie() ===
                false
26          -             && $this->authenticationService->getCurrentUser()->isAdmin() ===
                false) {
            26  +             || $this->authenticationService->getCurrentUser()->isAdmin() ===
                false) {
27      27                  return Response::createForbidden();
28      28              }
29      29
                @@ -66,7 +66,7 @@ public function deleteUser(Request $request) : Response
```

```
66  66      public function fetchUsers() : Response
67  67      {
68  68          if ($this->authenticationService->isUserAuthenticatedWithCookie() === false
69      -           && $this->authenticationService->getCurrentUser()->isAdmin() === false) {
    69  +           || $this->authenticationService->getCurrentUser()->isAdmin() === false) {
70  70              return Response::createForbidden();
71  71          }
72  72
```

Comments 0

Please sign in to comment.