reviactyl / **panel** Public

Code | Issues 12 | Pull requests | Discussions | Actions | Projects | S

Commit `fe0c29f`

aymenelouadi committed 4 days ago · ✓ 9 / 9

```
fix(auth): prevent OAuth account takeover via auto-linking

Remove automatic account linking when a social provider email matches
an existing user account. An attacker could create a social account
(Google/GitHub/Discord) using the victim's email address and gain
full access to their panel account without knowing their password.

The fix removes the auto-link logic entirely. Users who want to link
a social account must first log in with their email and password,
then manually link the provider from Account Settings.

Security: CVE-class Account Takeover via OAuth Auto-Link
```

develop (#297) · v26.2.0-beta.5

1 parent 676e8b0 commit fe0c29f

1 file changed +5 -17 lines changed

Top

Filter files…

app/Http/Controllers/Auth

SocialLoginController.php

1 file changed +5 -17 lines changed

Search within code

.../Controllers/Auth/SocialLoginController.php

```
@@ -83,23 +83,11 @@ public function callback(string $provider)
83  83              return redirect('/');
84  84          }
85  85
86      -       // Check if user with email exists (Auto-Link)
87      -       $user = User::where('email', $socialUser->getEmail())->first();
```

```
88  -
89  -         if ($user) {
90  -             // Link account automatically if email matches
91  -             $user->socialLogins()->create([
92  -                 'provider' => $provider,
93  -                 'provider_user_id' => $socialUser->getId(),
94  -                 'provider_token' => $socialUser->token,
95  -                 'provider_refresh_token' => $socialUser->refreshToken,
96  -             ]);
97  -
98  -             Auth::login($user);
99  -
100 -             return redirect('/');
101 -         }
102 -
        86  +         // If a user with the same email already exists, do NOT auto-link.
        87  +         // Auto-linking allows account takeover: an attacker could create a
        88  +         // social account using the victim's email and gain full access.
        89  +         // Instead, require the user to log in with their password first,
        90  +         // then manually link the social account from Account Settings.
103     91              return redirect()->route('auth.login')->with('error',
            trans('auth.social.not_linked', ['provider' => ucfirst($provider)]));
104     92          }
105     93
```

Comments 0

Please sign in to comment.