chamilo / **chamilo-lms** Public

Code | Issues 415 | Pull requests 12 | Discussions | Actions | Projects

Commit `0acf8a1`

AngelFQC committed 3 weeks ago · ✕ 0 / 3 · Verified

```
Security: Restrict non-admin users from modifying admin-only user fields in REST API

See advisory GHSA-3gqc-xr75-pcpw
```

1.11.x · v1.11.38

1 parent 866bd9f commit 0acf8a1

1 file changed +20 -1 lines changed

Top

Filter files…

main/inc/lib/webservices

Rest.php

1 file changed +20 -1 lines changed

Search within code

main/inc/lib/webservices/Rest.php

```
@@ -2707,10 +2707,26 @@ public function updateUserFromUserName(array $parameters): bool
2707 2707             throw new Exception(get_lang('NoData'));
2708 2708         }
2709 2709
2710      -         if (!api_is_platform_admin() && $userId != $this->user->getId()) {
     2710 +         $isAdmin = api_is_platform_admin();
     2711 +
     2712 +         if (!$isAdmin && $userId != $this->user->getId()) {
2711 2713             self::throwNotAllowedException();
2712 2714         }
2713 2715
```

```
                2716 +          // Fields that only platform admins may change
                2717 +          $adminOnlyFields = [
                2718 +              'status',
                2719 +              'roles',
                2720 +              'auth_source',
                2721 +              'enabled',
                2722 +              'active',
                2723 +              'creator_id',
                2724 +              'registration_date',
                2725 +              'expiration_date',
                2726 +              'hr_dept_id',
                2727 +              'official_code',
                2728 +          ];
                2729 +
2714            2730            if (!empty($parameters['new_login_name'])) {
2715            2731                // Make sure the new username, if set, is available
2716            2732                if
    (!UserManager::is_username_available($parameters['new_login_name'])) {
                                @@ -2732,6 +2748,9 @@ public function updateUserFromUserName(array
                                $parameters): bool
2732            2748
2733            2749            // apply submitted modifications
2734            2750            foreach ($parameters as $name => $value) {
                2751 +              if (!$isAdmin && in_array(strtolower($name), $adminOnlyFields,
                                    true)) {
                2752 +                  self::throwNotAllowedException();
                2753 +              }
2735            2754                switch (strtolower($name)) {
2736            2755                    case 'email':
2737            2756                        $user->setEmail($value);
```

Comments 0

Please sign in to comment.