Missing Authorization Check on User Group Removal via save-permissions Action

Moderate **angrybrad** published **GHSA-jq2f-59pj-p3m3** last week

Package

php **craftcms/cms** (Composer)

Affected versions

>= 5.6.0, <= 5.9.15

Patched versions

5.9.15

Description

Summary

The `actionSavePermissions()` endpoint allows a user with only `viewUsers` permission to remove arbitrary users from all user groups. While `_saveUserGroups()` enforces per-group authorization for additions, it performs no equivalent authorization check for removals, so submitting an empty `groups` value removes all existing group memberships.

Affected Versions

- Craft CMS 5.6.0 through 5.9.14 (latest release at time of report)
- Regression introduced in 5.6.0 when the `viewUsers` permission was added
- Prior to 5.6.0, `editedUser()` required `editUsers`, which implicitly protected this endpoint
- Requires Pro edition or higher (the vulnerable code path is gated by `CmsEdition::Pro`)

Vulnerability Details

Root Cause

This is a **regression** introduced in Craft CMS 5.6.0 when the `viewUsers` permission was added. Before that change, `editedUser()` required `editUsers` permission for accessing other users' data, which implicitly protected `actionSavePermissions()`. After the change, `actionSavePermissions()` became reachable for users with read-only access to other users, but the underlying group-saving logic still lacked authorization for group removals.

The vulnerability has two components:

1. **`actionSavePermissions()` reachable with read-only access**: The action only requires a control panel request and delegates to `editedUser()`, which now only checks `viewUsers` — a permission explicitly documented as "read-only access to user elements."

2. **Asymmetric authorization in `_saveUserGroups()`**: The method checks `assignUserGroup` permission only when **adding** a user to a new group. When the `groups` parameter is an empty string (resulting in an empty array), the loop is skipped entirely, no authorization checks are run, and all group memberships are removed.

Prerequisites

- Attacker has a control panel account with `accessCp` and `viewUsers` permissions only
- Target user belongs to one or more user groups that grant additional permissions
- Pro edition or higher

Attack Steps

1. Attacker authenticates to the Control Panel
2. Attacker sends a POST request to `actions/users/save-permissions` with:
   - `userId` = target user's ID
   - `groups` = `` (empty string)
3. All group memberships for the target user are removed
4. All permissions inherited from those groups are immediately revoked

Impact

- **Privilege revocation**: An attacker can strip group-based permissions from arbitrary users, including accounts whose effective access derives from group membership
- **Denial of access**: Users lose access to sections, volumes, and features that were granted through group membership
- **Bypass of elevated session requirement**: Group removal does not trigger `requireElevatedSession()` (which is only triggered when new groups are added)

References

`b135384`

Severity

Moderate

CVE ID

CVE-2026-41128

Weaknesses

▶ CWE-862

Credits

kaminuma Reporter