Redmine - Defect #11870

Users can delete their own accounts unconditionally via REST API

2012-09-18 21:30 - Enrique Castilla Contreras

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	REST API	**Estimated time:**	0.00 hour
Target version:	4.2.0		
Resolution:	Fixed	**Affected version:**	

Description

On Users collection, an administrator may delete its own account on Redmine, making it unusable.

Doing exploratory testing tasks with API REST I've accidentally deleted my own user on http://ecastillac.m.redmine.org, making the server unusable for me.

I've tried this script, provided Admin user had id=2 as shown in a previous execution:

```
#!/usr/bin/perl -w

use strict;
use warnings;

our ($VERSION) = '0.01'; # q$Revision$ =~ /(\d+)/;

use Test::More;
use Data::Dump;

# ------------------------------------------------

use Redmine::API;

my($API_Key, $BASE_URL) = do 'config';

my $api = Redmine::API->new( auth_key => $API_Key
                           , base_url => $BASE_URL
                           , trace => $ARGV[0] || 0);

my($res, $res1);

# ------------------------------------------------

#$res = $api->users->x->all();
#ddx $res->body;

$res1 = $api->users->user->del( 2 );
ddx $res1->body;
```

Associated revisions

Revision 20782 - 2021-03-13 08:20 - Go MAEDA

Fix that users can delete their own accounts unconditionally via REST API (#11870).

Patch by Mizuki ISHIKAWA and Kevin Fischer.

History

#1 - 2012-09-19 09:45 - Etienne Massip

I don't get why it would be a defect? Just don't delete your admin account if you have only one...

#2 - 2020-06-13 03:08 - Go MAEDA

The web UI does not allow admins to delete your account unconditionally.

- "Administration > Users" page always disallows users to delete their own account
- Users can delete their own account on My account page when the setting "Allow users to delete their own account" is enabled, but admins are allowed to delete their own account on the page only when there is another user with an admin privilege

So, I think API should not allow avoiding the limitations. The following code disallows admins to delete their own accounts via API or by sending a crafted request if "Allow users to delete their own account" is not enabled.

```
diff --git a/app/controllers/users_controller.rb b/app/controllers/users_controller.rb
index 2fb297874..578ac5a9a 100644
--- a/app/controllers/users_controller.rb
+++ b/app/controllers/users_controller.rb
@@ -184,6 +184,8 @@ class UsersController < ApplicationController
   end

   def destroy
+    raise Unauthorized if @user == User.current && !@user.own_account_deletable?
+
     @user.destroy
     respond_to do |format|
       format.html { redirect_back_or_default(users_path) }
```

#3 - 2020-06-25 08:55 - Mizuki ISHIKAWA

- File fix-11870.patch added

I've attached a patch based on #11870#note-2.
It was developed by pair programming with @kfischer_okarin.

#4 - 2020-06-26 01:18 - vzvu 3k6k

LGTM.

If I have to say something, it would be more user-friendly if the reason of the error is returned (such as "Can't delete your own account") with render_api_errors or something, but anyway it looks good to me.

#5 - 2020-06-28 09:08 - Go MAEDA

- Target version set to 4.2.0

Setting the target version to 4.2.0.

#6 - 2020-07-02 06:11 - Mizuki ISHIKAWA

- File fix-11870-v2.patch added

vzvu 3k6k wrote:

> LGTM.
>
> If I have to say something, it would be more user-friendly if the reason of the error is returned (such as "Can't delete your own account") with render_api_errors or something, but anyway it looks good to me.

Thank you for your feedback.
I changed to return error message.

@user.own_account_deletable? will be false if User.current was the last admin user. If there is an opinion that it is better to display another error message only in that case, I will improve the patch

#7 - 2020-07-13 09:47 - Go MAEDA

Mizuki ISHIKAWA wrote:

> vzvu 3k6k wrote:
>
> > LGTM.
> >
> > If I have to say something, it would be more user-friendly if the reason of the error is returned (such as "Can't delete your own account") with render_api_errors or something, but anyway it looks good to me.
>
> Thank you for your feedback.

> I changed to return error message.

I agree that returning an informative error message is user-friendly, however, I think the behavior is not consistent with other API responses. I prefer the first patch.

#8 - 2020-07-13 10:04 - Mizuki ISHIKAWA

Go MAEDA wrote:

> I agree that returning an informative error message is user-friendly, however, I think the behavior is not consistent with other API responses. I prefer the first patch.

Thanks for reviewing this patch!

Although there is no precedent that directly uses render_api_errors to return error messages, it is common to return validation error messages with render_validation_errors.
I don't think the behavior of the API from the user's perspective is that special.

And, in the case of exceptions that meet special conditions like this time, it is better to issue an error message even if it is different from other API responses.

I wrote it as above, but if the current specification makes it difficult to commit, I think it is better to prioritize the commit of the first patch!

#9 - 2020-07-13 11:13 - Kevin Fischer

I think for now it might be good to follow Redmine's current practice, i.e. no special error message.

But still it would be good to create another ticket (if one doesn't exist yet) to discuss/improve the general Rest API error response format of Redmine and adapt it to best practices for Rest APIs

#10 - 2020-07-14 18:39 - vzvu 3k6k

- File fix-11870-v3.patch added

Go MAEDA wrote:

> I agree that returning an informative error message is user-friendly, however, I think the behavior is not consistent with other API responses. I prefer the first patch.

Thank you for pointing it out.

Certainly most of (or all of?) Redmine APIs don't return error messages when deletion fails. I think it is because in most cases users can easily guess why their request failed. On the flip side, it might be worth returning a error message when it is difficult for users to guess why.

Maybe this should be discussed on another issue as Kevin Fischer says.

Mizuki ISHIKAWA wrote:

> @user.own_account_deletable? will be false if User.current was the last admin user. If there is an opinion that it is better to display another error message only in that case, I will improve the patch

I'm sorry for the late reply. Good catch, and thank you for writing another patch. I didn't think of it until you said.

As you suggest, I feel the message of "This user is your own user and cannot be deleted" can be confusing when the error reason is that User.current was the last admin user.

I've attached another patch to try to solve this confusion by adding another error message, though I'm not sure this API should return an error message for now.

#11 - 2021-03-13 08:24 - Go MAEDA

- Subject changed from REST API allows delete Admin user, making Redmine unusable to Users can delete their own accounts unconditionally via REST API

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed fix-11870.patch. Thank you for your contribution.

The following issues have been fixed in r20782:

- Users can delete their own account even when the setting "Allow users to delete their own account" is disabled
- An admin can delete their own account even if they are the last admin

Files

fix-11870.patch	1.46 KB	2020-06-25	Mizuki ISHIKAWA
fix-11870-v2.patch	3.54 KB	2020-07-02	Mizuki ISHIKAWA
fix-11870-v3.patch	1.54 KB	2020-07-14	vzvu 3k6k