

Redmine - Defect #32199

Security notification is not sent when an admin changes the password of a user

2019-10-05 04:06 - Go MAEDA

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Go MAEDA	% Done:	0%
Category:	Email notifications	Estimated time:	0.00 hour
Target version:	5.0.0	Affected version:	
Resolution:	Fixed		
Description			
Security notifications should be sent when admin changes a user's password in order to prevent admins from changing a user's password for malicious purposes.			
See the table below. It describes the current behavior. Security notifications for change of email address are sent even when the change is made by admins. However, security notifications for change of password are not sent if the change is made by admins. The behavior is inconsistent.			
	by the user	by admins	
Change of password	<input type="checkbox"/>	-	
Change of email address	<input type="checkbox"/>	<input type="checkbox"/>	

Associated revisions

Revision 21006 - 2021-05-24 08:28 - Go MAEDA

Security notification is not sent when an admin changes the password of a user (#32199).

Patch by Yuichi HARADA.

History

#1 - 2019-10-08 06:43 - Yuichi HARADA

- File [32199_change_password_by_admin.patch](#) added

Go MAEDA wrote:

Security notifications should be sent when admin changes a user's password in order to prevent admins from changing a user's password for malicious purposes.

+1

Security notification is send when an admin changes the password of users.

I attached a patch.

#2 - 2019-10-30 10:46 - Go MAEDA

- Target version set to Candidate for next major release

#3 - 2020-03-03 15:42 - Go MAEDA

- Target version changed from Candidate for next major release to 4.2.0

Setting the target version to 4.2.0.

#4 - 2020-08-22 09:19 - Go MAEDA

Thank you for posting the patch.

The patch [32199_change_password_by_admin.patch](#) does not send a security notification if one of the following conditions is met:

- The user is not active (e.g. locked)
- The current user changes their own password on /users/:id/edit page
- The checkbox "Send account information to the user" is checked

But I think a security notification should always be sent when an user's password has been changed. Assume the following situations. If security notifications are skipped in some conditions, a malicious person can secretly change someone's password:

- If a notification is not sent for a locked user, a malicious admin can secretly change an active user's password while temporarily lock the user
- If a notification is not sent when the current user's password is updated via `/users/:id/edit`, a malicious person can update the password secretly if the user has gone somewhere with the screen open
- If a notification is not sent when the checkbox "Send account information to the user" is checked, the behavior is inconsistent with the case the user's email is updated

#5 - 2020-08-24 08:17 - Yuichi HARADA

Go MAEDA wrote:

Thank you for posting the patch.

The patch [32199_change_password_by_admin.patch](#) does not send a security notification if one of the following conditions is met:

- The user is not active (e.g. locked)
- The current user changes their own password on `/users/:id/edit` page
- The checkbox "Send account information to the user" is checked

But I think a security notification should always be sent when an user's password has been changed. Assume the following situations. If security notifications are skipped in some conditions, a malicious person can secretly change someone's password:

- If a notification is not sent for a locked user, a malicious admin can secretly change an active user's password while temporarily lock the user
- If a notification is not sent when the current user's password is updated via `/users/:id/edit`, a malicious person can update the password secretly if the user has gone somewhere with the screen open
- If a notification is not sent when the checkbox "Send account information to the user" is checked, the behavior is inconsistent with the case the user's email is updated

Thank you for pointing out. I will revise the patch. Please wait for a while.

#6 - 2020-09-01 10:29 - Yuichi HARADA

- File `32199_change_password_by_admin-v2.patch` added

Yuichi HARADA wrote:

Thank you for pointing out. I will revise the patch. Please wait for a while.

I remade the patch. Unconditionally send a security notification when admin changes a user password.

```
diff --git a/app/controllers/users_controller.rb b/app/controllers/users_controller.rb
index 2fb297874..alc224f7a 100644
--- a/app/controllers/users_controller.rb
+++ b/app/controllers/users_controller.rb
@@ -145,7 +145,8 @@ class UsersController < ApplicationController
   end

   def update
-    if params[:user][:password].present? && (@user.auth_source_id.nil? || params[:user][:auth_source_id].blank?)
+    update_password = params[:user][:password].present? && (@user.auth_source_id.nil? || params[:user][:auth_source_id].blank?)
+    if update_password
       @user.password, @user.password_confirmation = params[:user][:password], params[:user][:password_confirmation]
     end
     @user.safe_attributes = params[:user]
@@ -157,6 +158,7 @@ class UsersController < ApplicationController
     if @user.save
       @user.pref.save

+      Mailer.deliver_password_updated(@user, User.current) if update_password
       if was_activated
         Mailer.deliver_account_activated(@user)
       elsif @user.active? && params[:send_information] && @user != User.current
```

#7 - 2021-03-25 08:32 - Marius BĂLTEANU

- Target version changed from 4.2.0 to 5.0.0

#8 - 2021-05-24 08:30 - Go MAEDA

- Subject changed from *Security notification is not sent when an admin changes the password of users* to *Security notification is not sent when an admin changes the password of a user*
- Status changed from *New* to *Closed*
- Assignee set to *Go MAEDA*
- Resolution set to *Fixed*

Committed the patch. Thank you for your contribution.

Security notifications will now also be sent when an admin changes a user's password.

Files

32199_change_password_by_admin.patch	2.88 KB	2019-10-08	Yuichi HARADA
32199_change_password_by_admin-v2.patch	2.63 KB	2020-09-01	Yuichi HARADA