Redmine - Defect #32192

Do not allow to send a security notification when the user account is locked.

2019-10-04 07:14 - Hinako Tajima

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Administration	**Estimated time:**	0.00 hour
Target version:			
Resolution:	Wont fix	**Affected version:**	

Description

I suggest that to add the function which if the account is locked, make disable to send security notifications.

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

History

#1 - 2019-10-04 07:19 - Go MAEDA

I could not confirm the behavior that locked users get security notifications. Could you describe the steps to reproduce?

#2 - 2019-10-04 09:26 - Hinako Tajima

Go MAEDA wrote:

> I could not confirm the behavior that locked users get security notifications. Could you describe the steps to reproduce?

This situation happens Ver.3.4.10, when the administrator saved after changed his/her email address who is a locked account.

#3 - 2019-10-04 15:59 - Go MAEDA

- Category set to Administration

Hinako Tajima wrote:

> This situation happens Ver.3.4.10, when the administrator saved after changed his/her email address who is a locked account.

I have confirmed that the trunk behaves the same. I think the notification should be sent even to locked users in order to prevent a malicious admin from abusing.

If security notifications are not sent to a locked user, a malicious admin can stealthily change an active user's email address with the following steps:

1. Lock the user
2. Change the email address of the user
3. Unlock the user

To prevent such illegal operation, security notifications should be sent to locked users if their user account is updated.

#4 - 2019-10-05 04:06 - Go MAEDA

- Subject changed from Do not allow to send a security mail when the user account is locked. to Do not allow to send a security notification when the user account is locked.

#5 - 2019-10-05 05:15 - Mischa The Evil

Go MAEDA wrote:

> I think the notification should be sent even to locked users [...]

I agree.

#6 - 2019-10-05 05:28 - Go MAEDA

- Status changed from New to Closed

- Resolution set to Wont fix

I am closing this as a "Wont fix" because the requested behavior change can be a security loophole.