Redmine - Defect #6254

Remove "Unknown user" notification on password request with non-existent email address

2010-08-31 11:48 - Aron Rotteveel

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Go MAEDA	**% Done:**	0%
Category:	Accounts / authentication	**Estimated time:**	0.00 hour
Target version:	5.1.0		
Resolution:	Fixed	**Affected version:**	

Description

Currently, it is possible to retrieve valid e-mailaddreses from the system by simply trying to request a password for it. If the emailaddress is not valid, Redmine will show a notification stating this.

It would be better to have this form output a success message in every scenario in order to make e-mail harvesting harder.

Related issues:

Has duplicate Redmine - Defect #25144: Account Harvesting login issue	**Closed**
Has duplicate Redmine - Defect #37517: User disclosure vulnerability via "For...	**Closed**

Associated revisions

Revision 22100 - 2023-02-07 04:53 - Go MAEDA

Remove "Unknown user" notification on password request with non-existent email address (#6254).

Patch by Go MAEDA.

History

#1 - 2017-02-22 02:22 - Go MAEDA

- Has duplicate Defect #25144: Account Harvesting login issue added

#2 - 2017-02-22 02:32 - Go MAEDA

source:tags/3.3.2/config/locales/en.yml#L153:

```
  notice_account_unknown_email: Unknown user.
```

#3 - 2017-02-22 02:39 - Go MAEDA

Aron Rotteveel wrote:

> It would be better to have this form output a success message in every scenario in order to make e-mail harvesting harder.

I completely agree. Redmine should always display notice_account_lost_email_sent ("An email with instructions to choose a new password has been sent to you.").

#4 - 2022-07-21 10:02 - j l

Hello,

I comment on this 12 years old defect because this is the only active one I found regarding this subject.
Is there a version in which this issue has been addressed, or a workaround ?

Thanks.
Regards,
JL

#5 - 2022-07-21 11:49 - Go MAEDA

- File 6254.patch added

The attached patch changes the message when the entered email address is invalid as follows. Comments are welcome.

Before: "Invalid user"
After: "An email with instructions to choose a new password has been sent to you"

#6 - 2022-07-28 16:54 - j l

This patch should indeed do the trick, thanks !

I would even suggest updating the message to more accurately reflect the reality. Something like "An email with instructions to choose a new password has been sent if the mail address matches an existing account"

#7 - 2022-08-11 00:43 - Mischa The Evil

- Has duplicate Defect #37517: User disclosure vulnerability via "Forgot password" functionality added

#8 - 2022-08-27 06:31 - Mischa The Evil

- Target version set to Unplanned backlogs

#9 - 2023-01-26 10:06 - Go MAEDA

- File 6254-v2.patch added

- Target version changed from Unplanned backlogs to 5.1.0

Setting the target version to 5.1.0.

#10 - 2023-02-07 04:52 - Go MAEDA

- Subject changed from Remove 'invalid user' notification on password request with invalid e-mailadress to Remove "Unknown user" notification on password request with non-existent email address

- Status changed from New to Closed

- Assignee set to Go MAEDA

- Resolution set to Fixed

Committed the patch.

#11 - 2023-10-29 23:50 - Mischa The Evil

- Start date deleted (2010-08-31)

Files

6254.patch	1.47 KB	2022-07-21	Go MAEDA
6254-v2.patch	42.3 KB	2023-01-26	Go MAEDA