Redmine - Feature #1415

Let system administrator limit repositories valid sources

2008-06-09 18:03 - Paul Rivier

Status:	Closed	**Start date:**	2008-06-09
Priority:	High	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	SCM	**Estimated time:**	0.00 hour
Target version:	3.0.0		
Resolution:	Fixed		

Description

As pointed out by Jean Philippe in #1393, users with project manager permissions can setup SCM sources to anything they want.
IOW, if they know any valid path to a repository in the hosting system, they can read it. It can be a serious privacy issue.
I think we should take some time to discuss it here, and find an elegant way to fix it.
What do you think about this ?

Related issues:

Related to Redmine - Feature #13038: Base path for filesystem repository adapter	**Closed**
Related to Redmine - Feature #17164: file:/// repository insecure	**Closed**
Has duplicate Redmine - Feature #10966: [SECURITY] Project Managers should no...	**Closed**
Has duplicate Redmine - Defect #18291: Path property security issue when addi...	**Closed**

Associated revisions

Revision 13573 - 2014-11-08 11:52 - Jean-Philippe Lang

Adds configuration settings to limit valid repository path (#1415).

Revision 13574 - 2014-11-08 11:53 - Jean-Philippe Lang

Adds text_subversion_repository_note string to locales (#1415).

History

#1 - 2008-06-09 18:07 - Paul Rivier

One possible design could be to restrict what a project manager can do from the Project Settings page. For exemple, we could disable 'modules' and 'repository' for non-admins. Very naïve solution.

#2 - 2008-06-10 08:36 - Anonymous

Does this not come down to trusting your managers. If you don't trust them, don't make them a project manager. Create another role with suitable privileges. The default roles only allows a developer to edit versions of a project.

Perhaps an explicit 'edit repository' to go along with the 'edit modules' setting could be added.

Cheers

Russell

#3 - 2008-06-10 09:51 - Jean-Philippe Lang

> Perhaps an explicit 'edit repository' to go along with the 'edit modules' setting could be added.

Actually, the permission already exists, it's called *Manage repository* (it lets user create/destroy the project's repository).

#4 - 2008-06-10 10:01 - Paul Rivier

Hi, Russel.

> Does this not come down to trusting your managers.

No. For an almost infinite number of reason, trust is never an acceptable argument when speaking about privacy or security. One example to illustrate

is : manager can give manager rights to other people. One other is : on common web application deployment, there is one person that administrates the hosting system, one other administrating redmine instance, and some people working on it with some privileges. Those people don't know each other. System administrator will probably use filesystem permissions to prevent redmine process from being able to visit the whole FS. But what can the redmine administrator do ? An instance is a single process with a single posix user, so it must be able to read all the repositories for all the projects. Some restriction facilities, at the redmine level, are probably missing.

> Perhaps an explicit 'edit repository' to go along with the 'edit modules' setting could be added.

Isn't that what 'manage repository' permission is about ?

#5 - 2008-06-11 06:33 - Anonymous

Hi Paul,

Just re-read your original report, and I completely miss-understood it yesterday so apologies for that. I can see the issue now.

> Isn't that what 'manage repository' permission is about ?

Ah yes, missed that one, was looking at the project group at the top.

Cheers

Russell

#6 - 2008-11-11 10:35 - Jean-Philippe Lang

- Target version deleted (0.8)

#7 - 2009-10-04 23:54 - Lluís Vilanova

- Status changed from New to Resolved

Unless I misunderstood the discussion, this is provided by the *Manage repository* permission, as previously commented.

#8 - 2013-01-15 22:38 - Jan Niggemann (redmine.org team member)

- Status changed from Resolved to Closed

Closing this, status is resolved since 400 days and more (issue was last updated more than 400 days ago)...

#9 - 2014-11-08 11:55 - Jean-Philippe Lang

- Subject changed from Let administrator limit repositories valid sources to Let system administrator limit repositories valid sources

- Status changed from Closed to Resolved

- Target version set to 3.0.0

- Resolution set to Fixed

r13573 lets you define regular expressions in the Redmine configuration file to limit valid repository path.

#10 - 2014-11-08 11:57 - Jean-Philippe Lang

- Has duplicate Feature #10966: [SECURITY] Project Managers should not be able to choose an URL for a local repository added

#11 - 2014-11-08 11:58 - Jean-Philippe Lang

- Related to Feature #13038: Base path for filesystem repository adapter added

#12 - 2014-11-08 11:59 - Jean-Philippe Lang

- Related to Feature #17164: file:/// repository insecure added

#13 - 2014-11-08 11:59 - Jean-Philippe Lang

- Has duplicate Defect #18291: Path property security issue when adding filesystem repository added

#14 - 2014-11-15 08:29 - Mischa The Evil

Woot! Nice to see this is added in this manner in 3.0.0. Thanks for it.

#15 - 2014-11-22 11:57 - Jean-Philippe Lang

- Status changed from Resolved to Closed