Redmine - Defect #13762

SCM auto status change bypassses roles and permissions

2013-04-14 08:28 - Marcus Rejås

Status:	Confirmed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	SCM	**Estimated time:**	0.00 hour
Target version:	Candidate for next major release		
Resolution:		**Affected version:**	

Description

Hi,

Encountered unexpected behavior yesterday when i accidentally added a Git archive cloned from another site (buildroot in this case) which contained a lot of commit-messages like

```
"Closes #1123"
```

This ended up in a lot of actions like:

```
Updated by Anonymous about 9 hours ago

    Status changed from New to Resolved
    % Done changed from 0 to 100

Comment Edit

Applied in changeset alleatoautomationplatform:buildroot|commit:4f0361ab2ca4f25207c84b557e31319c9a
417a76.
```

This was not only in the project the Repository is in but sitewide.

The user Anonymous have no permissions set.

This differs in two ways from my expected behavior:

1) The anonymous user should not be able to close issues.
2) A repo commit should only be able to modify issues in the same project as the repo.

This is an old installation that have gone through several upgrades. Unfortunately I don't have time to reproduce it in a clean environment but I thought it might be best reporting it anyway since it is security related.

```
Ruby version              1.9.3 (x86_64-linux)
RubyGems version          1.8.23
Rack version              1.4
Rails version             3.2.13
Active Record version     3.2.13
Action Pack version       3.2.13
Active Resource version   3.2.13
Action Mailer version     3.2.13
Active Support version    3.2.13
Middleware                Rack::Cache, ActionDispatch::Static, Rack::Lock, #<ActiveSupport::Cache:
::Strategy::LocalCache::Middleware:0x0000000289ede0>, Rack::Runtime, Rack::MethodOverride, ActionDi
spatch::RequestId, Rails::Rack::Logger, ActionDispatch::ShowExceptions, ActionDispatch::DebugExcep
tions, ActionDispatch::RemoteIp, ActionDispatch::Callbacks, ActiveRecord::ConnectionAdapters::Conn
ectionManagement, ActiveRecord::QueryCache, ActionDispatch::Cookies, ActionDispatch::Session::Cook
ieStore, ActionDispatch::Flash, RedmineDmsf::NoParse, ActionDispatch::ParamsParser, ActionDispatch
::Head, Rack::ConditionalGet, Rack::ETag, ActionDispatch::BestStandardsSupport, OpenIdAuthenticati
on
Application root          /var/www/redmine-2.2
Environment               production
Database adapter          mysql2
```

```
Database schema version   20121026003537
```

Thanks in advance and thank you for a great product. We love it!

Marcus

Related issues:

Related to Redmine - Feature #4823: Don't evaluate commit-message "refs, clos...	**New**	**2010-02-12**
Has duplicate Redmine - Defect #14276: Limit users than can reference and fix...	**Closed**	
Has duplicate Redmine - Defect #14826: Project permissions not respected in ...	**Closed**	
Has duplicate Redmine - Feature #13792: Fixing via git push should not break ...	**Closed**	

History

#1 - 2013-04-14 08:45 - Toshi MARUYAMA

- Category set to SCM

#2 - 2013-04-14 09:35 - Toshi MARUYAMA

- Status changed from New to Confirmed

- Target version set to 2.3.1

#3 - 2013-04-14 09:44 - Toshi MARUYAMA

- Target version changed from 2.3.1 to 2.4.0

#4 - 2013-04-14 10:03 - Toshi MARUYAMA

- Subject changed from Repositories bypassses roles and pesmissions to SCM auto status change bypassses roles and pesmissions

#5 - 2013-04-15 09:04 - Etienne Massip

I disagree with this one, Anonymous here is not the Redmine anonymous user but a developer **which has commit access** to the repository and which SCM identifier is not mapped to an actual Redmine user, this is far from being a lambda person but a member of the project.

This should not be touched IMHO.

#6 - 2013-04-15 11:13 - Marcus Rejås

Etienne Massip wrote:

> I disagree with this one, Anonymous here is not the Redmine anonymous user but a developer **which has commit access** to the repository and which SCM identifier is not mapped to an actual Redmine user, this is far from being a lambda person but a member of the project.
>
> This should not be touched IMHO.

I understand but it might lead to security breaches. You say that the person is being member of the project, but really it is member of *any* project. So if a committer by accident or on purpose mistypes the issue-id or enters one belonging to an external ticket system he or she might change things in a project where he or she might not have access. The person who made the mistake will not then be alerted at all and have no way to correct the problem.

My solution is to add three configuratoin options to the repos.

[] Allow altering of tickets through commit messages
[] Allow system wide altering of tickets through commit messages
[] Allow Non-mapped users in the repo to alter tickets through commit messages

We track external repos in some projects and this led to some confusion (to say the least) ...

#7 - 2013-06-16 13:07 - Toshi MARUYAMA

- Related to Defect #14276: Limit users than can reference and fix issues in commit messages added

#8 - 2013-06-18 08:43 - Toshi MARUYAMA

- Related to deleted (Defect #14276: Limit users than can reference and fix issues in commit messages)

#9 - 2013-06-18 08:44 - Toshi MARUYAMA

- Has duplicate Defect #14276: Limit users than can reference and fix issues in commit messages added

#10 - 2013-07-30 14:23 - Etienne Massip

- Subject changed from SCM auto status change bypassses roles and pesmissions to SCM auto status change bypassses roles and permissions

#11 - 2013-09-17 03:16 - Toshi MARUYAMA

- Has duplicate Defect #14826: Project permissions not respected in Fix/Reference commit added

#12 - 2013-10-13 10:14 - Jean-Philippe Lang

- Target version changed from 2.4.0 to Candidate for next major release

The root problem should be fixed by r4823 which disables issue updates when importing old commits. The requested option "Allow system wide altering of tickets through commit messages" is also already available as "Allow issues of all the other projects to be referenced and fixed".

#13 - 2013-10-14 00:33 - Mischa The Evil

Jean-Philippe Lang wrote:

> The root problem should be fixed by r4823 [...]

FTR: it should read *issue* #4823 (and r12199).

#14 - 2013-10-14 09:20 - Toshi MARUYAMA

- Related to Feature #4823: Don't evaluate commit-message "refs, closes, ..." when adding a repository added

#15 - 2015-12-30 06:50 - Go MAEDA

- Has duplicate Feature #13792: Fixing via git push should not break workflow added