ChiliProject - Feature # 1233: Bump rails to 2.3.17 to address [CVE-2013-0276]

Status:	Closed	**Priority:**	Normal
Author:	Milt Reder	**Category:**	Libraries
Created:	2013-02-11	**Assignee:**	Holger Just
Updated:	2013-02-13	**Due date:**	
Remote issue URL:			
Affected version:			
Description:	Description: https://groups.google.com/forum/?fromgroups=#!topic/rubyonrails-security/AFBKNY7VSH8 Rails team advises moving everything to attr_accessible, but the 2.3.17 patch is offered as a temporary fix.		

Associated revisions

2013-02-13 03:18 pm - Holger Just

Bump Rails to 2.3.17 #1233

2013-02-13 03:18 pm - Holger Just

Don't set YAML on serialized fields #1233

2013-02-13 03:18 pm - Holger Just

Remove monkey patch which is already included in Rails 2.3.17 #1233

2013-02-13 03:56 pm - Holger Just

Bump Rails to 2.3.17 #1233

2013-02-13 03:57 pm - Holger Just

Don't set YAML on serialized fields #1233

2013-02-13 03:58 pm - Holger Just

Remove monkey patch which is already included in Rails 2.3.17 #1233

History

2013-02-11 09:27 pm - Milt Reder

Realized the subject I put in for this issue is a little optimistic :P

Patching to 2.3.17 breaks a bunch of tests, example:

```
@  1) Error:
test_destroy_issue_attachment(AttachmentsControllerTest):
ActiveRecord::ActiveRecordError: You tried to assign already serialized content to changes. This is disabled due to security issues.
    app/models/issue.rb:371:in `attachment_removed'
    app/controllers/attachments_controller.rb:48:in `destroy'
    test/functional/attachments_controller_test.rb:113:in `test_destroy_issue_attachment'
    test/functional/attachments_controller_test.rb:112:in `test_destroy_issue_attachment'@
```

I guess this is a matter of getting rid of the remaining occurrences of attr_protected, so it's a big job:

```
/chiliproject/app/models/issue_relation.rb:
   39    validates_uniqueness_of :issue_to_id, :scope => :issue_from_id
   40
   41:   attr_protected :issue_from_id, :issue_to_id
```

```
  42
  43   def validate

/chiliproject/app/models/project.rb:
  64                 :author => nil
  65
  66:  attr_protected :status
  67
  68   validates_presence_of :name, :identifier

/chiliproject/app/models/query.rb:
  21   serialize :sort_criteria, Array
  22
  23:  attr_protected :project_id, :user_id
  24
  25   validates_presence_of :name, :on => :save

/chiliproject/app/models/role.rb:
  36
  37   serialize :permissions, Array
  38:  attr_protected :builtin
  39
  40   validates_presence_of :name

/chiliproject/app/models/time_entry.rb:
  22   belongs_to :activity, :class_name => 'TimeEntryActivity', :foreign_key => 'activity_id'
  23
  24:  attr_protected :project_id, :user_id, :tyear, :tmonth, :tweek
  25
  26   acts_as_customizable

/chiliproject/app/models/user.rb:
  58   attr_accessor :last_before_login_on
  59   # Prevents unauthorized assignments
  60:  attr_protected :login, :admin, :password, :password_confirmation, :hashed_password
  61
  62   validates_presence_of :login, :firstname, :lastname, :mail, :if => Proc.new { |user| !user.is_a?(AnonymousUser) }

/chiliproject/app/models/user_preference.rb:
  17   serialize :others
  18
  19:  attr_protected :others, :user_id
  20
  21   def initialize(attributes = nil)

/chiliproject/app/models/wiki_content.rb:
  72   # FIXME: This is for backwards compatibility only. Remove once we decide it is not needed anymore
  73   WikiContentJournal.class_eval do
  74:    attr_protected :data
  75     after_save :compress_version_text
  76

/chiliproject/app/models/repository/bazaar.rb:
  16
  17  class Repository::Bazaar < Repository
  18:   attr_protected :root_url
  19    validates_presence_of :url, :log_encoding
  20

/chiliproject/app/models/repository/filesystem.rb:
  16
  17  class Repository::Filesystem < Repository
  18:   attr_protected :root_url
  19    validates_presence_of :url
  20

/chiliproject/app/models/repository/git.rb:
  16
  17  class Repository::Git < Repository
  18:   attr_protected :root_url
  19    validates_presence_of :url
  20

/chiliproject/app/models/repository/mercurial.rb:
  19    has_many :changesets, :order => "#{Changeset.table_name}.id DESC", :foreign_key => 'repository_id'
  20
  21:   attr_protected :root_url
  22    validates_presence_of :url
  23

/chiliproject/app/models/repository/subversion.rb:
  16
  17  class Repository::Subversion < Repository
  18:   attr_protected :root_url
  19    validates_presence_of :url
  20    validates_format_of :url, :with => /^(http|https|svn(\+[^\s:\/\\]+)?|file):\/\/.+/i

/chiliproject/vendor/plugins/acts_as_watchable/lib/acts_as_watchable.rb:
  21                :conditions => ["#{Watcher.table_name}.user_id = ?", user_id] }
  22            }
  23:           attr_protected :watcher_ids, :watcher_user_ids
  24          end
  25        end

/chiliproject/vendor/plugins/awesome_nested_set/lib/awesome_nested_set.rb:
  76
  77          # no bulk assignment
  78:         attr_protected  left_column_name.intern,
  79                          right_column_name.intern,
  80                          parent_column_name.intern

/chiliproject/vendor/plugins/classic_pagination/test/fixtures/company.rb:
   1  #-- encoding: UTF-8
   2  class Company < ActiveRecord::Base
   3:   attr_protected :rating
   4    set_sequence_name :companies_nonstd_seq
```

5

2013-02-11 10:58 pm - Milt Reder

Totally forgot about the whole safe_attributes thing (silly of me, as I've used it in a plugin). I guess pretty big changes are required.

Background:
https://www.chiliproject.org/boards/2/topics/68
https://www.chiliproject.org/issues/655

2013-02-11 11:00 pm - Holger Just

Thanks for the notification. We are already investigating the issue.

The failing test you mentioned is not caused by @attr_accessible@ but because we pass serialized YAML from the controller down to the model which is forbidden since 2.3.17.

2013-02-11 11:01 pm - Holger Just

The @attr_accessible@ stuff that is already in there should not be of any actual concern to the security issue.

2013-02-11 11:02 pm - Milt Reder

Ah, so it was. Thanks!

Holger Just wrote:

> Thanks for the notification. We are already investigating the issue.
>
> The failing test you mentioned is not caused by @attr_accessible@ but because we pass serialized YAML from the controller down to the model which is forbidden since 2.3.17.

2013-02-13 03:17 pm - Holger Just

- Target version set to 3.7.0

- Assignee set to Holger Just

- Category set to Libraries

2013-02-13 07:35 pm - Holger Just

- Status changed from Open to Closed