

Redmine - Defect #14819

Newlines in attachment filename causes crash

2013-09-02 18:36 - Felix Schäfer

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Jean-Philippe Lang	% Done:	0%
Category:	Attachments	Estimated time:	0.00 hour
Target version:	2.4.0	Affected version:	2.3.1
Resolution:	Fixed		
Description			
<p>The routes for attachments require the filenames to conform to <code>/*</code> (see source:/branches/2.3-stable/config/routes.rb#L270). Unfortunately, this RegEx doesn't match newlines, which can occur in filenames of attachments. This causes actions with views showing attachments with full paths, for example using source:/branches/2.3-stable/app/helpers/application_helper.rb#L88, to crash.</p> <p>Sadly, it is not possible to use a multiline RegEx (<code>/*m</code>) to also match newlines in routes constraints, the best way we (Planio) have found to work around this is to use a negative match group with just <code>:[^\n]*/</code>. <code>/</code> are not allowed in filenames, and the routes constraint thus allows everything but a <code>.</code></p>			
Patch:			
<pre>--- a/config/routes.rb +++ b/config/routes.rb @@ -264,8 +264,8 @@ RedmineApp::Application.routes.draw do get 'projects/:id/repository', :to => 'repositories#show', :path => nil # additional routes for having the file name at the end of url - get 'attachments/:id/:filename', :to => 'attachments#show', :id => /\d+/, :filename => /*/, :as => 'named_attachment' - get 'attachments/download/:id/:filename', :to => 'attachments#download', :id => /\d+/, :filename => /*/, :as => 'download_named_attachment' + get 'attachments/:id/:filename', :to => 'attachments#show', :id => /\d+/, :filename => /^[^\n]*/ , :as => 'named_attachment' + get 'attachments/download/:id/:filename', :to => 'attachments#download', :id => /\d+/, :filename => /^[^\n]*/ , :as => 'download_named_attachment' get 'attachments/download/:id', :to => 'attachments#download', :id => /\d+/ get 'attachments/thumbnail/:id(/:size)', :to => 'attachments#thumbnail', :id => /\d+/, :size => /\d+/, :as => 'thumbnail' resources :attachments, :only => [:show, :destroy]</pre>			

Associated revisions

Revision 12128 - 2013-09-11 21:19 - Jean-Philippe Lang

Strip eols from file names (#14819).

Revision 12129 - 2013-09-11 23:31 - Jean-Philippe Lang

Remove EOLs from attachments filename (#14819).

Revision 12130 - 2013-09-11 23:34 - Jean-Philippe Lang

Typo (#14819).

History

#1 - 2013-09-04 09:00 - Etienne Massip

- Category set to Attachments

- Target version set to Candidate for next major release

#2 - 2013-09-10 19:22 - Jean-Philippe Lang

The handling of filenames with new lines seems broken anyway. Shouldn't we remove new lines from filenames instead or in addition to this patch?

#3 - 2013-09-11 13:54 - Felix Schäfer

I wouldn't mind removing them, but that solves the problem only for new uploads. Existing uploads could be handled either by taking care of the routes as above, or by having a migration to normalize existing filenames of the DB.

#4 - 2013-09-11 21:38 - Jean-Philippe Lang

I'd prefer the migration:

```
Index: db/migrate/20130911193200_remove_eols_from_attachments_filename.rb
=====
--- db/migrate/20130911193200_remove_eols_from_attachments_filename.rb    (revision 0)
+++ db/migrate/20130911193200_remove_eols_from_attachments_filename.rb    (revision 0)
@@ -0,0 +1,12 @@
+class RemoveEolsFromAttachmentsFilename < ActiveRecord::Migration
+  def up
+    Attachment.where("filename like ? or filename like ?", "%\r%", "%\n%").each do |attachment|
+      filename = attachment.filename.to_s.tr("\r\n", "_")
+      Attachment.where(:id => attachment.id).update_all(:filename => filename)
+    end
+  end
+
+  def down
+    # nop
+  end
+end
```

If it works for you, I'll commit this fix.

#5 - 2013-09-11 21:43 - Felix Schäfer

Try `attachment.update_column(:filename, filename)`, other than that it should work.

The fix in itself is good for us, we don't care whether it's solved one way or the other :-). Thanks!

#6 - 2013-09-11 23:43 - Jean-Philippe Lang

- Status changed from New to Closed
- Assignee set to Jean-Philippe Lang
- Target version changed from Candidate for next major release to 2.4.0
- Resolution set to Fixed

Migration committed, thanks for the feedback.

About `#update_column`: I prefer to stick with raw updates in migrations. `#update_column` does the raw update in the same way and runs some code to reflect the change in the instance attributes. This is neither useful nor desirable in this migration.