Redmine - Defect #37030

Requests fail with "Can't verify CSRF token authenticity" in mail handler

2022-04-25 15:21 - Matthias Hörmann

Status:	Closed	**Start date:**	
Priority:	Normal	**Due date:**	
Assignee:	Marius BĂLTEANU	**% Done:**	0%
Category:	Email receiving	**Estimated time:**	0.00 hour
Target version:	5.0.1		
Resolution:	Fixed	**Affected version:**	5.0.0

Description

```
Environment:
  Redmine version                5.0.0.stable.21535
  Ruby version                   2.5.5-p157 (2019-03-15) [x86_64-linux-gnu]
  Rails version                  6.1.5
  Environment                    production
  Database adapter               Mysql2
  Mailer queue                   ActiveJob::QueueAdapters::AsyncAdapter
  Mailer delivery                sendmail
Redmine settings:
  Redmine theme                  Default
SCM:
  Subversion                     1.10.4
  Git                            2.33.1
  Filesystem
Redmine plugins:
  redmine_agile                  1.6.4
  redmine_checklists             3.1.21
  redmine_theme_changer          0.5.0
```

After updating our Redmine to 5.0.0 incoming mails do not work because rdm-mailhandler.rb Requests appear in production.log with the error

```
I, [2022-04-25T14:58:39.595827 #24841]  INFO -- : [apache-342-1650891519593965] Started POST "/mai
l_handler" for 2a01:4f8:1c1c:f222::1 at 2022-04-25 14:58:39 +0200
I, [2022-04-25T14:58:39.596608 #24841]  INFO -- : [apache-342-1650891519593965] Processing by Mail
HandlerController#index as HTML
I, [2022-04-25T14:58:39.596815 #24841]  INFO -- : [apache-342-1650891519593965]   Parameters: {"ke
y"=>"<removed for security reasons>", "email"=>"<removed for privacy reasons>", "allow_override"=>
"project,tracker,category,assigned_to,priority,start_date,due_date", "unknown_user"=>nil, "default
_group"=>nil, "no_account_notice"=>nil, "no_notification"=>nil, "no_permission_check"=>nil, "proje
ct_from_subaddress"=>nil, "issue"=>{"tracker"=>"Inbox"}}
W, [2022-04-25T14:58:39.596952 #24841]  WARN -- : [apache-342-1650891519593965] Can't verify CSRF
 token authenticity.
I, [2022-04-25T14:58:39.597158 #24841]  INFO -- : [apache-342-1650891519593965] Completed 422 Unpr
ocessable Entity in 0ms (ActiveRecord: 0.0ms | Allocations: 118)
F, [2022-04-25T14:58:39.598093 #24841] FATAL -- : [apache-342-1650891519593965]
[apache-342-1650891519593965] ActionController::InvalidAuthenticityToken (ActionController::Invali
dAuthenticityToken):
[apache-342-1650891519593965]
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/request_forgery_prote
ction.rb:211:in `handle_unverified_request'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/request_forgery_prote
ction.rb:243:in `handle_unverified_request'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/request_forgery_prote
ction.rb:238:in `verify_authenticity_token'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:427:in `block
in make_lambda'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:198:in `block
(2 levels) in halting'
[apache-342-1650891519593965] actionpack (6.1.5) lib/abstract_controller/callbacks.rb:34:in `block
 (2 levels) in <module:Callbacks>'
```

```
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:199:in `block
in halting'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:512:in `block
in invoke_before'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:512:in `each'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:512:in `invoke
_before'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:105:in `run_ca
llbacks'
[apache-342-1650891519593965] actionpack (6.1.5) lib/abstract_controller/callbacks.rb:41:in `proce
ss_action'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/rescue.rb:22:in `proc
ess_action'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/instrumentation.rb:34
:in `block in process_action'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/notifications.rb:203:in `bl
ock in instrument'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/notifications/instrumenter.
rb:24:in `instrument'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/notifications.rb:203:in `in
strument'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/instrumentation.rb:33
:in `process_action'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal/params_wrapper.rb:249
:in `process_action'
[apache-342-1650891519593965] activerecord (6.1.5) lib/active_record/railties/controller_runtime.r
b:27:in `process_action'
[apache-342-1650891519593965] actionpack (6.1.5) lib/abstract_controller/base.rb:165:in `process'
[apache-342-1650891519593965] actionview (6.1.5) lib/action_view/rendering.rb:39:in `process'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal.rb:190:in `dispatch'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_controller/metal.rb:254:in `dispatch'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/routing/route_set.rb:50:in `d
ispatch'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/routing/route_set.rb:33:in `s
erve'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/journey/router.rb:50:in `bloc
k in serve'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/journey/router.rb:32:in `each
'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/journey/router.rb:32:in `serv
e'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/routing/route_set.rb:842:in `
call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/tempfile_reaper.rb:15:in `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/etag.rb:27:in `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/conditional_get.rb:40:in `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/head.rb:12:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/http/permissions_policy.rb:22
:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/http/content_security_policy.
rb:19:in `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/session/abstract/id.rb:266:in `context'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/session/abstract/id.rb:260:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/cookies.rb:689:in
`call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/callbacks.rb:27:in
 `block in call'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/callbacks.rb:98:in `run_cal
lbacks'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/callbacks.rb:26:in
 `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/actionable_excepti
ons.rb:18:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/debug_exceptions.r
b:29:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/show_exceptions.rb
:33:in `call'
```

```
[apache-342-1650891519593965] railties (6.1.5) lib/rails/rack/logger.rb:37:in `call_app'
[apache-342-1650891519593965] railties (6.1.5) lib/rails/rack/logger.rb:26:in `block in call'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/tagged_logging.rb:99:in `bl
ock in tagged'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/tagged_logging.rb:37:in `ta
gged'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/tagged_logging.rb:99:in `ta
gged'
[apache-342-1650891519593965] railties (6.1.5) lib/rails/rack/logger.rb:26:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/remote_ip.rb:81:in
 `call'
[apache-342-1650891519593965] request_store (1.5.1) lib/request_store/middleware.rb:19:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/request_id.rb:26:i
n `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/method_override.rb:24:in `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/runtime.rb:22:in `call'
[apache-342-1650891519593965] activesupport (6.1.5) lib/active_support/cache/strategy/local_cache_
middleware.rb:29:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/executor.rb:14:in
`call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/static.rb:24:in `c
all'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/sendfile.rb:110:in `call'
[apache-342-1650891519593965] rack (2.2.3) lib/rack/content_length.rb:17:in `call'
[apache-342-1650891519593965] actionpack (6.1.5) lib/action_dispatch/middleware/host_authorization
.rb:142:in `call'
[apache-342-1650891519593965] railties (6.1.5) lib/rails/engine.rb:539:in `call'
[apache-342-1650891519593965] /usr/lib/ruby/vendor_ruby/phusion_passenger/rack/thread_handler_exte
nsion.rb:107:in `process_request'
[apache-342-1650891519593965] /usr/lib/ruby/vendor_ruby/phusion_passenger/request_handler/thread_h
andler.rb:157:in `accept_and_process_next_request'
[apache-342-1650891519593965] /usr/lib/ruby/vendor_ruby/phusion_passenger/request_handler/thread_h
andler.rb:110:in `main_loop'
[apache-342-1650891519593965] /usr/lib/ruby/vendor_ruby/phusion_passenger/request_handler.rb:419:i
n `block (3 levels) in start_threads'
[apache-342-1650891519593965] /usr/lib/ruby/vendor_ruby/phusion_passenger/utils.rb:113:in `block i
n create_thread_and_abort_on_exception'
```

Since https://www.redmine.org/projects/redmine/wiki/redminereceivingemails does not mention anything about this and neither does the script I assume the script was not updated when this requirement was added?

Related issues:

Related to Redmine - Patch #36317: Set default protect from forgery true	**Closed**

Associated revisions

Revision 21568 - 2022-05-11 22:09 - Marius BĂLTEANU

Don't verify CSRF authenticity token in mail handler (#37030).

Patch by Go MAEDA.

Revision 21572 - 2022-05-12 07:55 - Marius BĂLTEANU

Merged r21568 to 5.0-stable (#37030).

History

#1 - 2022-04-25 15:49 - Matthias Hörmann

In addition to this rdm-mailhandler.rb also does not seem to fail with a proper exit code in this situation.

#2 - 2022-04-25 15:53 - Matthias Hörmann

It actually fails with exit code 77, there must be another reason then why it wasn't logged in my sieve.log unlike past errors.

#3 - 2022-04-26 14:00 - Matthias Hörmann

As a temporary fix I added

```
  def verify_authenticity_token
  end

  def handle_unverified_request
  end
```

to MailHandlerController (in app/controllers/mail_handler_controller.rb

This seems to work but I am not sure about the exact implications (I know neither Ruby nor Rails nor the Redmine codebase nor whether CSRF is actually needed in this context).

#4 - 2022-04-26 14:05 - Marius BĂLTEANU

- Assignee set to Marius BĂLTEANU

#5 - 2022-05-11 16:17 - Go MAEDA

It seems to be caused by r21379.

#6 - 2022-05-11 17:23 - Go MAEDA

- File 37030.patch added

I think the attached patch fixes the issue.

#7 - 2022-05-11 22:06 - Marius BĂLTEANU

- Target version set to 5.0.1

#8 - 2022-05-11 22:09 - Marius BĂLTEANU

- Status changed from New to Resolved

- Resolution set to Fixed

Fix committed, thanks!

#9 - 2022-05-12 05:00 - Go MAEDA

- Related to Patch #36317: Set default protect from forgery true added

#10 - 2022-05-12 07:56 - Marius BĂLTEANU

- Subject changed from rdm-mailhandler.rb Requests fail with "Can't verify CSRF token authenticity" to Requests fail with "Can't verify CSRF token authenticity" in mail handler

- Status changed from Resolved to Closed

#11 - 2022-10-13 22:39 - Aleksandar Pavic

Same problem is with issue_relations_controller.rb I have fixed it by adding
skip_before_action :verify_authenticity_token

However my Redmine was: 4.1.0

Files

37030.patch	1.12 KB	2022-05-11	Go MAEDA