# Redmine - Defect #12727

## CVE-2012-5664

2013-01-03 19:42 - Alex Shulgin

| | | | |
|---|---|---|---|
| **Status:** | Closed | **Start date:** | |
| **Priority:** | High | **Due date:** | |
| **Assignee:** | | **% Done:** | 0% |
| **Category:** | Rails support | **Estimated time:** | 0.00 hour |
| **Target version:** | | | |
| **Resolution:** | Fixed | **Affected version:** | 2.2.0 |

**Description**

Rails-3.2.9 needs to be updated to 3.2.10 in Gemfile.

### History

#### #1 - 2013-01-03 22:24 - Etienne Massip

*- Target version set to Candidate for next minor release*

*- Private changed from No to Yes*

Related to Comment on Recent Rails vulnerability.

#### #2 - 2013-01-03 23:57 - Jean-Philippe Lang

*- Target version changed from Candidate for next minor release to 2.2.1*

trunk upgraded to 3.2.10 in r11109.

#### #3 - 2013-01-05 10:31 - Toshi MARUYAMA

Merged to 2.2-stable by r11111.

#### #4 - 2013-01-08 22:50 - Jean-Baptiste Barth

I saw comments on various blog posts / tweets saying that the article mentionned in the forum thread is not accurate and the problem could be exploited without knowing the secret token. Btw, none of the code related to authentication is affected (there's already a params[:blah].to_s performed on user inputs everywhere, which is a workaround mentionned on rails blog post). So I'm 99% sure your Redmine instance is totally unaffected if you force authentication.

Unfortunately there are other security vulnerabilities regarding params in rails core pipe. One disclosed tonight may affect Redmine in some way, I'll open a different issue for that one.

#### #5 - 2013-01-09 09:05 - Etienne Massip

*- Status changed from New to Closed*

*- Target version deleted (2.2.1)*

*- Resolution set to Fixed*

Superseded by #12776 and upgrade to 3.2.11.

#### #6 - 2013-01-09 17:51 - Etienne Massip

*- Private changed from Yes to No*