Redmine - Defect #9567

Redmine.pm potential security issue with cache credential enabled and subversion

2011-11-14 20:40 - Guillaume Perréal

Status:	Closed	**Start date:**	2011-11-14
Priority:	High	**Due date:**	
Assignee:	Jean-Philippe Lang	**% Done:**	0%
Category:	SCM extra	**Estimated time:**	0.00 hour
Target version:	1.2.3		
Resolution:	Fixed	**Affected version:**	

Description

Redmine.pm credential cache is based only on project, user and password, ignoring permissions (or at least read/write type). Credentials cached for reading can thus be reused for committing.

Simple test case:

1. ensure credential cache is enabled using "RedmineCacheCredsMax 50",
2. create a private project with Subversion SCM,
3. assign an user with role "reviewer" (he should have only :browse_repository permission),
4. check out the project,
5. modify a file,
6. commit.

Here is log excerpt (user bob is reviewer of project monprojet):

First attempt, we get an error 401, asking the user to authenticate for read method "OPTIONS":

```
192.168.56.1 - - [14/Nov/2011:20:32:27 +0100] "OPTIONS /svn/monprojet/trunk HTTP/1.1" 401 762 "-"
"SVN/1.6.12 (r955767) neon/0.29.6"
```

Then the user successfully authenticates as bob, which is allowed read methods (OPTIONS and PROPFIND):

```
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "OPTIONS /svn/monprojet/trunk HTTP/1.1" 200 870 "-
" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "PROPFIND /svn/monprojet/trunk HTTP/1.1" 207 856 "
-" "SVN/1.6.12 (r955767) neon/0.29.6"
```

There comes the committing part, starting with MKACTIVITY, a **write** method:

```
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "MKACTIVITY /svn/monprojet/!svn/act/7d5d2d10-22bb-
429d-99d3-958c04a83f6c HTTP/1.1" 201 579 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "CHECKOUT /svn/monprojet/!svn/vcc/default HTTP/1.1
" 201 595 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "PROPPATCH /svn/monprojet/!svn/wbl/7d5d2d10-22bb-4
29d-99d3-958c04a83f6c/3 HTTP/1.1" 207 625 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "PROPFIND /svn/monprojet/trunk HTTP/1.1" 207 564 "
-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "CHECKOUT /svn/monprojet/!svn/ver/3/trunk HTTP/1.1
" 201 603 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "PROPFIND /svn/monprojet/!svn/wrk/7d5d2d10-22bb-42
9d-99d3-958c04a83f6c/trunk/bla3 HTTP/1.1" 404 503 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "PROPFIND /svn/monprojet/trunk/bla3 HTTP/1.1" 404
457 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "PUT /svn/monprojet/!svn/wrk/7d5d2d10-22bb-429d-99
d3-958c04a83f6c/trunk/bla3 HTTP/1.1" 201 602 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "MERGE /svn/monprojet/trunk HTTP/1.1" 200 1183 "-"
 "SVN/1.6.12 (r955767) neon/0.29.6"
192.168.56.1 - bob [14/Nov/2011:20:32:35 +0100] "DELETE /svn/monprojet/!svn/act/7d5d2d10-22bb-429d
-99d3-958c04a83f6c HTTP/1.1" 204 141 "-" "SVN/1.6.12 (r955767) neon/0.29.6"
```

Associated revisions

Revision 7809 - 2011-11-14 23:11 - Jean-Philippe Lang

Fixed: Redmine.pm potential security issue with cache credential enabled and subversion (#9567).

Revision 8120 - 2011-12-07 22:58 - Jean-Philippe Lang

Merged r7809 from trunk (#9567).

History

#1 - 2011-11-14 22:47 - Jean-Philippe Lang

- Status changed from New to Confirmed

Yes, RedmineCacheCredsMax should be disabled for now.

#2 - 2011-11-14 23:11 - Jean-Philippe Lang

- Status changed from Confirmed to Resolved

- Assignee set to Jean-Philippe Lang

- Resolution set to Fixed

This should be fixed in r7809. Can you confirm?

#3 - 2011-11-15 00:37 - Guillaume Perréal

Confirmed. It indeed denies MKACTIVITY in this test case.

#4 - 2011-11-15 22:16 - Jean-Philippe Lang

- Target version set to 1.2.3

#5 - 2011-12-07 22:59 - Jean-Philippe Lang

- Status changed from Resolved to Closed

Merged.