Redmine - Defect #4448
Subversion password cleanly visible in the process list and some logs

2009-12-18 17:10 - Holger Just

Status:	New	**Start date:**	2009-12-18
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	SCM	**Estimated time:**	0.00 hour
Target version:			
Resolution:		**Affected version:**	

Description

When using a remote Subversion repository which requires a password, that password is readable in the system's process list as well as in the developer log. This is because Redmine uses the system-installed svn binaries which to my knowledge do only accept passwords with a command-line parameter. As the complete command line of every running process is freely visible to every (potentially malicious) other process on the same system, that process can gather the subversion credentials used by Redmine.

Unfortunately, the only complete fix which comes to my mind is to use the SWIG bindings to svn itself instead of the binary.

In short terms, we should at least mask the password in the log files which are normally written to disk world-readable. This is done using the supplied patch.

This patch leads to the following output of the development log during a RepositoriesController#show:

```
  Processing RepositoriesController#show (for 127.0.0.1 at 2009-12-18 17:10:34) [GET]
    Parameters: {"action"=>"show", "id"=>"testproject", "controller"=>"repositories"}
    SQL (0.1ms)   SELECT max("settings".updated_on) AS max_updated_on FROM "settings"
    AnonymousUser Load (0.3ms)   SELECT * FROM "users" WHERE ( ("users"."type" = 'AnonymousUser' ) ) LIMIT 1
    Setting Load (0.1ms)   SELECT * FROM "settings" WHERE ("settings"."name" = 'login_required') LIMIT 1
    Project Load (0.2ms)   SELECT * FROM "projects" WHERE ("projects"."identifier" = 'testproject') LIMIT 1
    Repository Load (0.2ms)   SELECT * FROM "repositories" WHERE ("repositories".project_id = 1) LIMIT 1
    EnabledModule Load (0.4ms)   SELECT * FROM "enabled_modules" WHERE ("enabled_modules".project_id = 1)
    Role Load (0.2ms)   SELECT * FROM "roles" WHERE ("roles"."builtin" = 2) LIMIT 1
    Setting Load (0.1ms)   SELECT * FROM "settings" WHERE ("settings"."name" = 'autofetch_changesets') LIMIT 1
  Shelling out: svn info --xml 'https://example.com/svn/' --username xxxx --password xxxx --no-auth-cache --non-interactive
    Changeset Load (15.5ms)   SELECT * FROM "changesets" WHERE ("changesets".repository_id = 1) ORDER BY
  changesets.committed_on DESC, changesets.id DESC LIMIT 1
  Shelling out: svn list --xml 'https://example.com/svn/'@HEAD --username xxxx --password xxxx --no-auth-cache
  --non-interactive
  Found 3 entries in the repository for 'https://example.com/svn/'
  Shelling out: svn log --xml -r HEAD:1 --username xxxx --password xxxx --no-auth-cache --non-interactive --limit 10
  'https://example.com/svn/'
    Changeset Load (1.1ms)   SELECT * FROM "changesets" WHERE ("changesets"."revision" IN ('12','11','10','9','8','7','6','5',
  '4','3')) AND ("changesets".repository_id = 1) ORDER BY committed_on DESC, changesets.committed_on DESC,
  changesets.id DESC
  Shelling out: svn --version
  Shelling out: svn proplist --verbose --xml 'https://example.com/svn/'@HEAD --username xxxx --password xxxx --no-auth-cache
  --non-interactive
  Rendering template within layouts/base
  Rendering repositories/show
  Rendered redmine_checkout_hooks/_view_repositories_show_contextual (351.3ms)
  Rendered repositories/_navigation (13.2ms)
  Rendered repositories/_breadcrumbs (1.7ms)
```

Related issues:

Related to Redmine - Feature # 1536: Using libsvn	**New**	**2008-06-27**

Associated revisions

Revision 3251 - 2009-12-26 17:20 - Jean-Philippe Lang

Fixed: Subversion password visible in development logs (#4448).

History

#1 - 2009-12-18 18:11 - Holger Just

- File strip_scm_credentials_from_logs.patch added

Forgot the patch...

#2 - 2009-12-20 16:14 - Jean-Philippe Lang

- Category set to SCM

#3 - 2009-12-26 17:16 - Jean-Philippe Lang

Patch applied in r3251.
There's still the process list problem, see #1536 for using libsvn.

Files

strip_scm_credentials_from_logs.patch	665 Bytes	2009-12-18	Holger Just