Katello - Bug #6921

Non root/sudo users can execute some commands for katello-disconnected

08/04/2014 07:03 PM - Partha Aji

Status:	Closed		
Priority:	Normal		
Assignee:	Mike McCune		
Category:	Inter Server Sync		
Target version:	Katello 2.0		
Difficulty:	easy	**Fixed in Releases:**	
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:	1024107	**Red Hat JIRA:**	
Pull request:	https://github.com/Katello/katello-misc/pull/36		

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1024107
Description of problem:

Non-root user cannot run all commands for katello-disconnected, but can apparently execute enough that it can cause some minor havoc

Version-Release number of selected component (if applicable):

How reproducible:

Steps to Reproduce:
1. create a new user, 'loser'
2. su - loser
3. As 'loser', run the setup command with appropriate oauth-key and oauth-secret, as viewble in /etc/pulp/server.conf.
4. attempt to run various katello-disconnected commands.

Actual results:
Some commands fail similar to:

[loser@hp-dl380pgen8-02-vm-15 ~]$ katello-disconnected list
Red Hat Repositories
/usr/share/katello-disconnected/lib/disconnected_pulp.rb:43:in `list': undefined method `enabled_repositories' for nil:NilClass (NoMethodError)
from /usr/bin/katello-disconnected:455:in `<main>'

Others, though, apparently do not! Comamands that seem to work:
katello-disconnected sync
katello-disconnected export (mostly works)
katello-disconnected clean

Note that running 'clean' tended to muff up my katello-disconnected stuff for future syncs (admin and non-admin alike), though that may be a different issue unrelated to privileges .

Expected results:
Probably shouldn't allow this.
Should pulp's server.conf be readable only by root/sudo?
Possibly make katello-disconnected only +x by root/sudo, though i guess nothing stops someone from being able to create a script from source.
Not sure if we want to handle that NoMethodError by non priv user to indicate they probably shouldn't be doing this.

Additional info:

History

#1 - 08/04/2014 07:07 PM - Mike McCune

https://github.com/Katello/katello-misc/pull/36

#2 - 08/04/2014 10:07 PM - Eric Helms

- Category changed from Web UI to Inter Server Sync

- Target version set to 54

- Difficulty set to easy

- Triaged changed from No to Yes

- Pull request https://github.com/Katello/katello-misc/pull/36 added

- Pull request deleted ()

#3 - 08/15/2014 01:24 PM - Eric Helms

- Status changed from New to Closed

#4 - 08/22/2014 09:25 AM - Eric Helms

- translation missing: en.field_release set to 13