Foreman - Bug #25191

Canned admin role gives non-admin users access to settings

10/12/2018 03:23 PM - Michael Johnson

Status:	Resolved		
Priority:	High		
Assignee:			
Category:	Security		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

After canned admin role was added to Foreman (https://projects.theforeman.org/issues/24259) users without admin roles are able to access settings eventhough they should not be allowed to (https://github.com/xprazak2/foreman/blob/f01787b7f03d323309622013ad2fccd06ff75d8a/db/seeds.d/020-roles_list.rb#L91).

For example, when logged in as a user with the default "Viewer" role permissions, if I access the following url, the OAuth consumer key is returned along with other information: https://<HOSTNAME>.com/api/v2/settings/oauth_consumer_key

History

#1 - 10/12/2018 05:48 PM - Marek Hulán

Thanks for the report. Could you please checker, whether user has also other roles, content of default role permissions and most importantly, Viewers' role filter for Setting resource, whether it contains view-settings permission.

#2 - 10/12/2018 07:08 PM - Michael Johnson

Hey Marek, turns out, I didn't do a rake db:seed, so view_settings was still sitting in my default "Viewer" role. I just tested again and I can't view any settings. Sorry about the confusion here.

#3 - 10/12/2018 07:10 PM - Michael Johnson

- Status changed from New to Resolved