Foreman - Bug #24851

Do not allow users to escalate their own permissions

09/07/2018 12:53 PM - Ondřej Pražák

Status:	New		
Priority:	Low		
Assignee:			
Category:	Users, Roles and Permissions		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

It is possible for users to escalate their own permissions and gain access to additional actions/resources. So far, I have discovered the following scenarios where it occurs:

Scenario A
1) Have a non-admin user in OrgA and LocA with a Manager role
2) User can add more organizations to himself

Scenario B
1) Have a non-admin user with all permissions for Role and Filter
2) User can add a new filter to the role he already owns.

Scenario C
1) Have a non-admin user with all permissions to Usergroup
2) User can add himself to the usergroup

Related issues:

Related to Foreman - Bug #7222: a user should be prevented from creating a ro...	**Rejected**	**08/21/2014**

History

#1 - 09/10/2018 01:23 PM - Marek Hulán

I'm not sure how expected this is but this is the meaning of "assign_organizations" (scenario A), "create_roles" and "create_filters" (scenario B), "create_usergroups" + "update_users" permission (scenario C). These permissions should be only granted to users who need them.

I think this was already opened once at https://projects.theforeman.org/issues/7222 but closed since the implementation was not accepted. Perhaps we could reuse that ticket for escalation handling or at least for inspiration.

#2 - 09/10/2018 01:23 PM - Marek Hulán

- Related to Bug #7222: a user should be prevented from creating a role filter that exceeds their own filters added

#3 - 09/10/2018 01:23 PM - Marek Hulán

- Category set to Users, Roles and Permissions

#4 - 09/11/2018 07:13 AM - Ondřej Pražák

- Assignee deleted (Ondřej Pražák)

- Priority changed from Normal to Low

Marek Hulán wrote:

> I'm not sure how expected this is but this is the meaning of "assign_organizations" (scenario A), "create_roles" and "create_filters" (scenario B), "create_usergroups" + "update_users" permission (scenario C). These permissions should be only granted to users who need them.
>
> I think this was already opened once at https://projects.theforeman.org/issues/7222 but closed since the implementation was not accepted. Perhaps we could reuse that ticket for escalation handling or at least for inspiration.

I absolutely agree that permissions should be granted only to users who need them. My main concern is that these permissions allow users to become more powerful by adding permissions to themselves. I do not think users should decide about what permissions they have and get more when they feel like it. If they do not have them when their account was set up, then they probably do not need them. And if they do, they should be delegated by another person.

The #7222 is related to scenario B, but different. It says that I can only create new role with filters for hosts if I have filters for hosts. Scenario B does not care what roles/filters I create when I have permissions to do it, it just does not want to permit modifying role I already own with additional filter.

But this seems as a low priority at the moment.