pfSense - Bug #5294

System users and groups not fully protected from deletion

10/10/2015 02:35 PM - Fernando Munoz

Status:	Resolved	**Start date:**	10/10/2015
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	User Manager / Privileges	**Estimated time:**	0.00 hour
Target version:	2.2.5		
Affected Version:	All	**Affected Architecture:**	

Description

It's possible to shoot yourself on the foot and delete the admin user and all/admin groups.

1. Configure tamper data/ burpsuit

Delete admin user - Steps to reproduce
2. Create any user
3. Attempt to delete that user and modify the http request, put user id 0 and name admin
4. admin will be deleted

Delete all/admins groups
2. Create a group called all or admins
3. Attempt to delete the group created and modify thehttp request, put group id 0 if using all or 1 if using admins
4. group will be deleted

This checks should be applied on the server side before attempting to do the action and not just when showing the menu.

History

#1 - 10/11/2015 03:13 AM - Phillip Davis

https://github.com/pfsense/pfsense/pull/1957 should check for this case of the user manually messing with the $POST value of "id" and display an input error message rather than deleting a system user.
I guess something similar for the Groups tab will cover that case also.

#2 - 10/11/2015 03:38 AM - Phillip Davis

https://github.com/pfsense/pfsense/pull/1958
Similar fix for preventing deletion of a system group.

#3 - 10/11/2015 03:39 AM - Phillip Davis

If these fixes for RELENG_2_2 are accepted, then they need to also be done in master for 2.3

#4 - 10/12/2015 11:45 AM - Phillip Davis

System User Delete checks committed https://github.com/pfsense/pfsense/commit/8d070c072ec2b662f6a235cc3779fb62835dd647
System Group Delete checks committed https://github.com/pfsense/pfsense/commit/d7e5efa46134e738ae62e5c387c1e92fd803124d

This should be fixed in a RELENG_2_2 snapshot built after the time of this post.

@Fernando - please test with these changes and confirm that these system users and groups are now protected from deletion.

#5 - 10/13/2015 09:15 PM - Chris Buechler

- Subject changed from Deleting the undeletable to System users and groups not fully protected from deletion

- Category set to User Manager / Privileges

- Status changed from New to Feedback

- Target version set to 2.2.5

- Affected Version set to All

#6 - 10/20/2015 07:54 PM - Chris Buechler

- Status changed from Feedback to Resolved

fixed