Foreman - Refactor #21267

Remove dangerous send from power API

10/10/2017 07:16 AM - Lukas Zapletal

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Power management		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

We are using inputs as symbols with send method for power operations, this is dangerous. It is not a security issue at the moment as our permissions require edit or power permissions for all operations, but we should prevent that. Creating a safe_send method could do the trick, we'd need to check if the method is allowed from a list of methods.

Confidence: High
Category: Dangerous Send
Check: Send
Message: User controlled method execution
Code: host.power.send(params[:power][:action].to_sym)
File: app/controllers/hosts_controller.rb
Line: 475

Confidence: High
Category: Dangerous Send
Check: Send
Message: User controlled method execution
Code: (resource_base.friendly.find(params[:id]) or
resource_base.find_by_mac(params[:host][:mac].to_s)).power.send(params[:powe
r_action].to_sym)
File: app/controllers/hosts_controller.rb
Line: 266