Installer - Bug #12646

Isolated Reverse proxy exposes all of Katello/Foreman

12/01/2015 09:32 AM - Travis Camechis

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

Description

After doing some investigation, The Client hits hits the reverse proxy on the capsule at 8443 and it gets proxied to the backend Katello instance. If from a browser I actually hit the url for instance (https://capsule:8443/); It actually takes me directly to the foreman box and that looks to be how the reverse proxy is setup on an isolated capsule. That seems to be somewhat of a security hole since your exposing the full Katello instance to the outside. I modified to the reverse proxy to only proxy /rhsm urls and that seems to be a little better and subscription management still works. There are apis that are displayed in JSON format when I hit the URL now but at least its not the foreman application itself. I am not sure if there is a better solution to this? Would it be possible maybe to host a small RHSM client on the capsule that forwards the request back to Katello? Just thoughts

I have attached the proxy config I used.

Related issues:

Related to Katello - Feature #17367: Capsule should listen for RHSM requests ...	**New**	**11/16/2016**

History

#1 - 12/21/2015 09:32 AM - Eric Helms

- translation missing: en.field_release set to 86

- Triaged changed from No to Yes

#2 - 04/18/2016 09:23 AM - Eric Helms

- translation missing: en.field_release changed from 86 to 143

#3 - 07/08/2016 11:37 AM - Justin Sherrill

- Category set to Installer

- translation missing: en.field_release changed from 143 to 114

- Difficulty set to easy

This is expected behavior, but i could see allowing the user to specify a slimmed down set of actions to allow, possibly defaulting to that.

#4 - 02/14/2018 06:48 PM - Justin Sherrill

- translation missing: en.field_release changed from 114 to 338

#5 - 06/19/2018 06:42 PM - Stephen Benjamin

- Related to Feature #17367: Capsule should listen for RHSM requests on port 443, like Satellite does added

#6 - 06/19/2018 06:43 PM - Stephen Benjamin

If #17367 were fixed in the proposed way (only proxy /rhsm on 443), it would also solve this and I think #17367 has had more complaints.

#7 - 07/11/2018 06:27 PM - Justin Sherrill

- Target version changed from Katello 3.7.0 to Katello 3.8.0

- Triaged set to No

#8 - 08/20/2018 01:17 PM - Eric Helms

- Target version deleted (Katello 3.8.0)

- Triaged changed from Yes to No

#9 - 08/22/2018 05:56 PM - Andrew Kofink

- Target version set to Katello Backlog

- Triaged changed from No to Yes

#10 - 03/05/2020 06:35 PM - Anthony Chevalet

Hi there, any news about this "security hole"?

#11 - 05/17/2021 11:00 PM - Eric Helms

We have assessed this bug and there are a few considerations. The reverse proxy on the content proxy grants both UI and API access which in our view has the same security implications. In order to lock down just to the API we would have to build an access list of **all** API paths needed in order to not break functionality. Given there is no single rooted endpoint this is difficult and has the potential to miss an endpoint and break functionality. Additionally, some users see this as a feature that they use in order to access the application from clients or the content proxy itself. Given all of this, it is our recommendation that we close this bug as rejected.

#12 - 08/09/2023 11:28 AM - Ewoud Kohl van Wijngaarden

- Project changed from Katello to Installer

- Category deleted (Installer)

- Target version deleted (Katello Backlog)

We've merged katello-installer into foreman-installer and for better visibility I'm moving it over to the installer project.

Files

28-katello-reverse-proxy.conf	1.96 KB	12/01/2015	Travis Camechis