Smart Proxy - Feature #6677

Autosign entry additions should require authentication

07/17/2014 03:18 PM - Michael Messmore

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

Description

Using the smart proxy API, I can create an autosign entry by POSTing to http://smartproxy.example.com/puppet/ca/autosign/NAME without any authentication. There should be some type of trust relationship established between the client and the Smart Proxy on the CA (cert, OAuth, user/password, whatever) to prevent unauthorized users from being able to get the CA to sign a key.

This isn't the end of the world, but it does break the trust model in the CA to have untrusted things able to get the CA to sign keys.

I was able to reproduce this on Foreman 1.5.1, and assume it is always that way (hopefully not making an ass out of anyone).

Related issues:

Related to Smart Proxy - Bug #7822: CVE-2014-3691 - Smart proxy doesn't perfo...	**Closed**	**10/06/2014**

History

#1 - 10/06/2014 06:43 AM - Dominic Cleal

- Related to Bug #7822: CVE-2014-3691 - Smart proxy doesn't perform verification of client SSL certificate on API requests added

#2 - 10/08/2014 06:46 AM - Dominic Cleal

We're fixing the requirement for SSL verification in #7822, but you give an HTTP example - are you running with or without SSL? I guess we could put in some authentication for the HTTP-only mode.

#3 - 10/28/2014 09:29 PM - Michael Messmore

Yeah, sorry that was a typo. I can confirm that the behavior I observed is fixed in 1.5.4, because I was forced to add the cert to the request. Thanks!

#4 - 10/29/2014 04:31 AM - Dominic Cleal

- Status changed from New to Resolved

Ah great, thanks for the report.