Foreman - Bug #12314

Foreman does not work with FIPS enabled

10/26/2015 02:37 PM - Kendall Moore

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

Description

With FIPS mode enabled, Foreman won't run. Results are as follows:

foreman-rake apiepie:cache
Apipie cache enabled but not present yet. Run apipie:cache rake task to speed up API calls.
md5_dgst.c(80): OpenSSL internal error, assertion failed: Digest MD5 forbidden in FIPS mode!
/tmp/tmp.mrjvUccRvF: line 1: 25276 Aborted rake apipie:cache

Specifically this is because MD5 is not a valid cipher with FIPS enabled. After some digging, it seems that stems from Rack.
Check here: https://github.com/rack/rack/blob/master/lib/rack/etag.rb#L2
And here: https://github.com/rack/rack/blob/master/lib/rack/etag.rb#L68

Hopefully there aren't many cipher issues but I can't continue to find out until this one gets resolved.

Related issues:

Is duplicate of Foreman - Feature #3511: As a security person, I would like ...	**Resolved**

History

#1 - 10/27/2015 04:38 AM - Dominic Cleal

- Is duplicate of Feature #3511: As a security person, I would like Foreman to run in FIPS mode added

#2 - 10/27/2015 04:39 AM - Dominic Cleal

- Status changed from New to Duplicate

Thanks for the report. We're tracking this under ticket #3511 since it's the older ticket, but I'll add a note there as your observations are valuable. If you come across anything else, please add it to that ticket - cheers.