Smart Proxy - Bug #17783

foreman-proxy exposes server version in header

12/19/2016 04:09 PM - Andrew Kofink

Status:	Duplicate		
Priority:	Normal		
Assignee:			
Category:			
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1404867	**Red Hat JIRA:**	
Pull request:			

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1404867
Description of problem:

```
foreman-proxy sends back a "Server" header with http requests, exposing the version of webrick and
 openssl.

Nessus will claim that the server is suseptable to CVEs that have already been backported into ope
nssl, since it performs its check based on the reported version and not the release. For example,
1.0.1e-60 has a lot of fixes backported, but nessus only sees "1.0.1e" and complains.

While this particular behavior is a nessus issue, it is generally better to not report the server'
s openssl version in the header in the first place.

Version-Release number of selected component (if applicable): 6.2.4, foreman-proxy-1.11.0.6-1.el7s
at.noarch,

How reproducible: every time

Steps to Reproduce:
 1. curl -v http://&amp;lt;hostname&amp;gt;:8000
 2. look for Server header in response

Actual results:

< Server: WEBrick/1.3.1 (Ruby/2.0.0/2015-12-16) OpenSSL/1.0.1e

Expected results:

blank field, or no field at all

Additional info:

This is very similar to upstream issue https://github.com/theforeman/smart-proxy/pull/402
 which is waiting on the contributor for an update.

the following simple patch to /usr/share/foreman-proxy/lib/launcher.rb seems to do the trick:

--- launcher.rb 2016-12-14 16:44:44.245330301 -0500
 +++ launcher.rb.new     2016-12-14 16:44:33.002000676 -0500
 @ -28,6 +28,7 @
          :Host => SETTINGS.bind_host,
          :Port => SETTINGS.http_port,
          :Logger => ::Proxy::LogBuffer::Decorator.instance,
 +        :ServerSoftware => "",
          :daemonize => false)
      end
```

```
@ -57,6 +58,7 @@
             :SSLCertificate => load_ssl_certificate(SETTINGS.ssl_certificate),
             :SSLCACertificateFile => SETTINGS.ssl_ca_file,
             :SSLOptions => ssl_options,
 +           :ServerSoftware => "",
             :daemonize => false)
         end
       end
```

History

#1 - 12/20/2016 02:32 AM - Shlomi Zadok

- Project changed from Katello to Smart Proxy

- Subject changed from foreman-proxy exposes server version in header to foreman-proxy exposes server version in header

- Category deleted (Foreman Proxy Content)

- Status changed from New to Duplicate

Duplicate of #14394