Smart Proxy - Bug #7822
CVE-2014-3691 - Smart proxy doesn't perform verification of client SSL certificate on API requests
10/06/2014 06:39 AM - Dominic Cleal

Status: Closed
Priority: Urgent
Assignee: Dominic Cleal
Category: SSL
Target version: 1.5.4
Difficulty:

Pull request: https://github.com/theforeman/smart-proxy/pull/217

Triaged:

Bugzilla link:

Description
Reported to foreman-security by Michael Moll. Also reported by Jon McKenzie in a comment here: http://projects.theforeman.org/issues/5651#note-1, and possibly the same as Michael Messmore's #6677 ticket.

The smart proxy when running in an SSL-secured mode permits incoming API calls to any endpoint without requiring, or performing any verification of an SSL client certificate. This permits any client with access to the API to make requests and perform actions (permitting control of Puppet CA, DHCP, DNS etc.)

Users are strongly recommended to ensure smart proxy ports (typically 8443/tcp) are firewalled so only Foreman hosts can access the service and to set the "trusted_hosts" config setting in /etc/foreman-proxy/settings.yml to a list of Foreman hostnames for host based access control.

See https://groups.google.com/forum/#!topic/foreman-announce/jXC5ixybjqo for more information on mitigation.

Related issues:
- Related to Smart Proxy - Feature #6677: Autosign entry additions should require authentication
- Related to Smart Proxy - Refactor #7832: Integration test for SSL verification
- Related to Smart Proxy - Feature #7849: trusted_hosts should determine hostnames
- Related to Installer - Bug #8301: Add a checker script for reverse DNS
- Has duplicate Smart Proxy - Bug #5651: The 'trusted_hosts' config key has an unintuitive (and potentially dangerous) behavior

Associated revisions
Revision 52f0bacf - 10/08/2014 08:26 AM - Dominic Cleal
fixes #7822 - forbid HTTPS requests with no client SSL certificate

History
#1 - 10/06/2014 06:39 AM - Dominic Cleal
- Project changed from Foreman to Smart Proxy
- Category changed from Security to SSL

#2 - 10/06/2014 06:40 AM - Dominic Cleal
- Has duplicate Bug #5651: The 'trusted_hosts' config key has an unintuitive (and potentially dangerous) behavior

#3 - 10/06/2014 06:43 AM - Dominic Cleal
- Related to Feature #6677: Autosign entry additions should require authentication

#4 - 10/06/2014 07:22 AM - Dominic Cleal
- Status changed from New to Assigned
- Assignee set to Dominic Cleal
#5 - 10/07/2014 07:01 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/smart-proxy/pull/217 added
- Pull request deleted ()

#6 - 10/07/2014 07:34 AM - Dominic Cleal
- Related to Refactor #7832: Integration test for SSL verification added

#7 - 10/08/2014 05:13 AM - Dominic Cleal
- Related to Feature #7849: trusted_hosts should determine hostname from certificate CN on SSL requests added

#8 - 10/08/2014 07:46 AM - Dominic Cleal
- Description updated

#9 - 10/08/2014 07:47 AM - Dominic Cleal
- Legacy Backlogs Release (now unused) set to 26

#10 - 10/08/2014 09:01 AM - Dominic Cleal
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset 5f0badf26923826a9b112369d504972369bb3cf0.

#11 - 10/08/2014 10:41 AM - Dominic Cleal
We plan on releasing updated foreman-proxy packages as part of 1.5.4 and 1.6.2.

#12 - 10/09/2014 03:13 AM - Dominic Cleal
- Subject changed from Smart proxy doesn't perform verification of client SSL certificate on API requests to CVE-2014-3691 - Smart proxy doesn't perform verification of client SSL certificate on API requests

1.5-stable commit: https://github.com/theforeman/smart-proxy/commit/a4ecc166f7f86de63d68a66d677eef3d6d4c8193.patch
1.6-stable commit: https://github.com/theforeman/smart-proxy/commit/d3def6c43e24bdde105e15add2fc74b4950bba55.patch

The 1.5-stable patch should apply cleanly on 1.2 to 1.4 too.

#13 - 10/09/2014 05:28 AM - Dominic Cleal
1.5.4 and 1.6.2 have been shipped: https://groups.google.com/forum/#!topic/foreman-announce/LcjZx25Bl7U

#14 - 11/06/2014 07:35 AM - Dominic Cleal
- Related to Bug #8301: Add a checker script for reverse DNS added