## CVE-2017-2667 - SSL/HTTPS server certificates are not verified by default

03/27/2017 07:55 AM - Dominic Cleal

<table>
<thead>
<tr>
<th>Status:</th>
<th>Closed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority:</td>
<td>Normal</td>
</tr>
<tr>
<td>Assignee:</td>
<td>Tomáš Strachota</td>
</tr>
<tr>
<td>Category:</td>
<td>Hammer core</td>
</tr>
<tr>
<td>Target version:</td>
<td></td>
</tr>
<tr>
<td>Difficulty:</td>
<td></td>
</tr>
<tr>
<td>Triaged:</td>
<td>No</td>
</tr>
<tr>
<td>Bugzilla link:</td>
<td></td>
</tr>
<tr>
<td>Pull request:</td>
<td></td>
</tr>
<tr>
<td>Team Backlog:</td>
<td></td>
</tr>
<tr>
<td>Fixed in Releases:</td>
<td></td>
</tr>
<tr>
<td>Found in Releases:</td>
<td></td>
</tr>
<tr>
<td>In Kanboard:</td>
<td></td>
</tr>
</tbody>
</table>

### Description

HTTPS connections initiated by Hammer to the API server do not perform validation of the server SSL/TLS certificate, allowing for a man-in-the-middle attack against the user.

#12400 has introduced automatic certificate verification when an SSL CA is explicitly configured, but the default for HTTPS connections remains off. It could be verified against the system CA store.

Reported by Tomas Strachota to foreman-security@googlegroups.com.

### Related issues:

- Related to Hammer CLI - Bug #12400: Missing option to enable verification of the server certificate.
- Closed 11/05/2015

### Associated revisions

**Revision 081a0a40 - 03/28/2017 10:16 AM - Tomas Strachota**

Refs #19033 - Instructions for fetching SSL CA cert (#293)

- Refs #19033 - Instructions for fetching SSL CA cert

**Revision 74b926ae - 03/28/2017 10:23 AM - Tomas Strachota**

Fixes #19033 - Enable SSL verification by default (#235)

- Fixes #19033 - Enable SSL verification by default
- Refs #19033 - Option for fetching server CA cert

### History

**#1 - 03/27/2017 07:55 AM - Dominic Cleal**

- Related to Bug #12400: Missing option to enable verification of the server certificate. added

**#2 - 03/27/2017 09:40 AM - Dominic Cleal**

- Subject changed from SSL/HTTPS server certificates are not verified by default to CVE-2017-2667 - SSL/HTTPS server certificates are not verified by default
#3 - 03/27/2017 09:45 AM - Tomáš Strachota
- Status changed from New to Assigned
- Assignee set to Tomáš Strachota

#4 - 03/28/2017 07:07 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/hammer-cli/pull/235 added

#5 - 03/28/2017 07:07 AM - The Foreman Bot
- Pull request https://github.com/theforeman/hammer-cli-foreman/pull/293 added

#6 - 03/28/2017 11:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset 74b926ae24f471d93b778e06b64935a57b60e33.