Foreman - Bug #5436
CVE-2014-0192 - provisioning templates are world accessible
04/24/2014 08:01 PM - Ohad Levy

Status: Closed
Priority: Normal
Assignee: Ohad Levy
Category: Unattended installations
Target version: 1.4.4
Difficulty: 

Pull request: 
Fixed in Releases: 
Found in Releases: 1.4.0

Description
since 1e0fd283 it is possible to override spoof by providing a hostname parameters.
this would allow to retrieve any template of any host bypassing authentication.

Related issues:
Has duplicate Foreman - Bug #5463: No authentication required for /unattended...

Duplicate 04/26/2014

Associated revisions
Revision aa0be8e - 04/28/2014 10:56 AM - Ohad Levy
fixes #5436 - provisioning templates are world accessible

Revision 8abee388 - 04/28/2014 11:51 AM - Ohad Levy
fixes #5436 - provisioning templates are world accessible
(cherry picked from commit aa0be8eef311875695135c1714cb09225e8cd13)

Revision 09659e1e - 04/29/2014 08:37 AM - Ohad Levy
fixes #5436 - provisioning templates are world accessible
(cherry picked from commit aa0be8eef311875695135c1714cb09225e8cd13)

History

#1 - 04/24/2014 08:08 PM - Ohad Levy
a simple example using curl:

curl http://0.0.0.0:3000/unattended/provision/?hostname=abc

#2 - 04/24/2014 10:38 PM - Dominic Cleal

Hm, I think I see from the code - we're only applying the authorisation filters when the spoof parameter isn't used, in the assumption that this is the only parameter needing protection. Bit messy.
This has probably been in since 5b70f0e0 / #359, so Foreman 1.4.0 and above are affected.
#3 - 04/28/2014 08:03 AM - Dominic Cleal
- Private changed from Yes to No

Removing private flag as it's been reported publicly.

#4 - 04/28/2014 08:03 AM - Dominic Cleal
- Has duplicate Bug #5463: No authentication required for /unattended/provision?hostname=HOSTNAME added

#5 - 04/28/2014 08:35 AM - Ohad Levy
- Status changed from New to Ready For Testing
- Assignee set to Ohad Levy

https://github.com/theforeman/foreman/pull/1404

#6 - 04/28/2014 11:31 AM - Ohad Levy
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset aa0ebe8eef311875695135c1714cb09225e8cd13.

#7 - 04/29/2014 07:52 AM - Dominic Cleal
- Subject changed from provisioning templates are world accessible to CVE-2014-0192 - provisioning templates are world accessible

#8 - 04/29/2014 10:50 AM - Dominic Cleal
- Legacy Backlogs Release (now unused) changed from 4 to 17

Fix available in 1.5.0-RC2 and above.