Foreman - Bug #15490

CVE-2016-4995 - view_hosts permissions/filters not checked for provisioning template previews

06/22/2016 05:44 AM - Dominic Cleal

Status:	Closed		
Priority:	Normal		
Assignee:	Lukas Zapletal		
Category:	Security		
Target version:	1.11.4		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.11.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/2428		

Description

Users who are logged in with permissions to view some hosts are able to preview provisioning templates for any host by specifying its hostname in the URL, as the specific view_hosts permissions and filters aren't checked. If the organization or location features are enabled, the user will still be restricted to their associated orgs/locs.

This can disclose configuration information about the host, including root password hashes if used in preseed/kickstart templates.

Foreman versions 1.11.0 and higher are vulnerable.

Related issues:

Related to Foreman - Refactor #13039: Remove DB queries from class of Unatten...	**Closed**	**01/07/2016**
Related to Foreman - Bug #10689: Unattended controller permission check does ...	**Duplicate**	**06/03/2015**

Associated revisions

Revision c3c186de - 07/13/2016 07:40 AM - Lukas Zapletal

Fixes #15490 - adding view_host filter and better msg

Users who are logged in with permissions to view some hosts are able to preview provisioning templates for any host by specifying its hostname in the URL, as the specific view_hosts permissions and filters aren't checked. If the organization or location features are enabled, the user will still be restricted to their associated orgs/locs.

This can disclose configuration information about the host, including root password hashes if used in preseed/kickstart templates.

Revision 9abcd03b - 07/22/2016 10:03 AM - Lukas Zapletal

Fixes #15490 - adding view_host filter and better msg

Users who are logged in with permissions to view some hosts are able to preview provisioning templates for any host by specifying its hostname in the URL, as the specific view_hosts permissions and filters aren't checked. If the organization or location features are enabled, the user will still be restricted to their associated orgs/locs.

This can disclose configuration information about the host, including root password hashes if used in preseed/kickstart templates.

(cherry picked from commit c3c186de12be15e55d9582e54659f765304a1073)

Revision e638c374 - 07/22/2016 10:05 AM - Lukas Zapletal

Fixes #15490 - adding view_host filter and better msg

Users who are logged in with permissions to view some hosts are able to preview provisioning templates for any host by specifying its hostname in the URL, as the specific view_hosts permissions and filters aren't checked. If the organization or location features are enabled, the user will still be restricted to their associated orgs/locs.

This can disclose configuration information about the host, including
root password hashes if used in preseed/kickstart templates.

(cherry picked from commit c3c186de12be15e55d9582e54659f765304a1073)

History

#1 - 06/22/2016 05:44 AM - Dominic Cleal

- Related to Refactor #13039: Remove DB queries from class of UnattendedController added

#2 - 06/22/2016 05:45 AM - Dominic Cleal

- Related to Bug #10689: Unattended controller permission check does not work added

#3 - 06/22/2016 06:06 AM - Dominic Cleal

This vuln was introduced by #13039, but the patch for #10689 (which itself is now resolved) should serve to fix the issue when the ticket number's updated.

#4 - 06/22/2016 06:59 AM - Dominic Cleal

- Subject changed from view_hosts permissions/filters not checked for provisioning template previews to CVE-2016-4995 - view_hosts permissions/filters not checked for provisioning template previews

#5 - 07/12/2016 03:17 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Lukas Zapletal

#6 - 07/12/2016 06:11 AM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/2428 added

#7 - 07/13/2016 08:01 AM - Lukas Zapletal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset c3c186de12be15e55d9582e54659f765304a1073.