Discovery - Bug #10469
Auto provision rule does not enforce host group association to org/location

05/11/2015 10:55 AM - Dominic Cleal

Status: Closed
Priority: Normal
Assignee: Lukas Zapletal
Category: Discovery plugin
Target version:
Difficulty: Pull request: https://github.com/theforeman/foreman_discovery/pull/202
Triaged: No
Bugzilla link:

Description
This was reported by Ori Rabin to foreman-security (thanks!) and a CVE identifier was filed under CVE-2015-3199, but it turned out this does not affect any released upstream version.

Steps to reproduce:

1. log in with a user that has 2 locations (A, B)
2. discover a host and make sure it is connected to location B
3. create a hostgroup in location A
4. create a discovery rule in location B to match the discovered host and use the hostgroup from 3
5. log in with a user with permissions to location B only
6. you can see in the discovery rules index page the rule with the hostgroup you created (you can't access the hostgroup)
7. auto provision the discovered host
8. go to hosts - the host was provisioned using a hostgroup the second user doesn't have permissions for

The rule creation should enforce that the selected host group is in the same org/location as the rule itself.

Optionally Discovery could also enforce that users must have view_hostgroups permissions for their target host group when using rules, but this isn't done in Foreman core today anyway - #4477, #6470 etc.

Related issues:
Related to Discovery - Bug #9881: Discovery rules are not connected to taxonomy
Closed 03/24/2015

Associated revisions
Revision 5cb015eb - 08/11/2015 06:22 AM - Lukas Zapletal
Fixes #10469 - enforced discovery rule taxonomy

History

#1 - 05/11/2015 10:59 AM - Dominic Cleal
- Description updated

#2 - 05/13/2015 05:22 AM - Dominic Cleal
- Subject changed from Auto provision rule does not enforce host group association to org/location to CVE-2015-3199 - Auto provision rule does not enforce host group association to org/location
- Description updated

#3 - 05/19/2015 11:52 AM - Dominic Cleal
Given #9881's not even in Discovery 2.x or 3.0.0, does this actually affect any released software? AFAICT, it doesn't.

#4 - 05/21/2015 09:12 AM - Lukas Zapletal
I can confirm this was not yet released:

g branch -r --contains 47ecc19a26809dabca37aa8d43231aebebde4351dc | grep origin
origin/HEAD -> origin/develop
origin/develop

#5 - 05/21/2015 09:27 AM - Lukas Zapletal
- Related to Bug #9881: Discovery rules are not connected to taxonomies added

#6 - 05/21/2015 09:31 AM - Lukas Zapletal
- Subject changed from CVE-2015-3199 - Auto provision rule does not enforce host group association to org/location to Auto provision rule does not enforce host group association to org/location
- Description updated

Updated subject and description.

#7 - 07/23/2015 10:43 AM - Lukas Zapletal
- Status changed from New to Assigned
- Assignee set to Lukas Zapletal

#8 - 07/24/2015 06:25 AM - The Foreman Bot
- Status changed from Assigned to Ready For Testing
- Pull request https://github.com/theforeman/foreman_discovery/pull/202 added
- Pull request deleted ()

#9 - 08/11/2015 07:01 AM - Anonymous
- Status changed from Ready For Testing to Closed
- % Done changed from 0 to 100

Applied in changeset foreman_discovery|5cb015eb6ab9be490956af00300bddd1df94c8d18.