Foreman - Bug #15653

CVE-2016-5390 - access to API host interfaces, parameters etc. are not restricted by view_hosts filters

07/12/2016 03:57 AM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Daniel Lobato Garcia		
Category:	Users, Roles and Permissions		
Target version:	1.11.4		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.10.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/3644		

Description

Non-admin users with the view_hosts permission containing a filter are able to access API routes beneath "hosts" such as GET /api/v2/hosts/secrethost/interfaces without the filter being taken into account. This allows users to access network interface details (including BMC login details) for any host.

The filter is only correctly used when accessing the main host details (/api/v2/hosts/secrethost). Access to the "nested" routes, which includes interfaces, reports, parameters, audits, facts and Puppet classes, is not authorized beyond requiring any view_hosts permission.

Affects Foreman 1.10.0 and higher.

Reported by Daniel Lobato Garcia, Nacho Barrientos and Steve Traylen to foreman-security@googlegroups.com.

CVE identifier will be requested.

Related issues:

Related to Foreman - Bug #8343: API resource_scope ignores options	**Closed**	**11/11/2014**
Related to Foreman - Bug #16219: Association named 'hostgroup' was not found ...	**Closed**	**08/22/2016**

Associated revisions

Revision 7a86dcfe - 07/19/2016 08:27 AM - Daniel Lobato Garcia

Fixes #15653 - CVE-2016-5390 fix permissions for host API

Non-admin users with the view_hosts permission containing a filter are able to access API routes beneath "hosts" such as GET /api/v2/hosts/secrethost/interfaces without the filter being taken into account. This allows users to access network interface details (including BMC login details) for any host.

The filter is only correctly used when accessing the main host details (/api/v2/hosts/secrethost). Access to the "nested" routes, which includes interfaces, reports, parameters, audits, facts and Puppet classes, is not authorized beyond requiring any view_hosts permission.

Revision 82d33af2 - 07/22/2016 10:49 AM - Daniel Lobato Garcia

Fixes #15653 - CVE-2016-5390 fix permissions for host API

Non-admin users with the view_hosts permission containing a filter are able to access API routes beneath "hosts" such as GET /api/v2/hosts/secrethost/interfaces without the filter being taken into account. This allows users to access network interface details (including BMC login details) for any host.

The filter is only correctly used when accessing the main host details (/api/v2/hosts/secrethost). Access to the "nested" routes, which includes interfaces, reports, parameters, audits, facts and Puppet

classes, is not authorized beyond requiring any view_hosts permission.

(cherry picked from commit 7a86dcfe6b36dd43cd6163ce70599e53f09cc217)

Revision 020fdac4 - 07/22/2016 10:50 AM - Daniel Lobato Garcia

Fixes #15653 - CVE-2016-5390 fix permissions for host API

Non-admin users with the view_hosts permission containing a filter are
able to access API routes beneath "hosts" such as GET
/api/v2/hosts/secrethost/interfaces without the filter being taken into
account. This allows users to access network interface details
(including BMC login details) for any host.

The filter is only correctly used when accessing the main host details
(/api/v2/hosts/secrethost). Access to the "nested" routes, which
includes interfaces, reports, parameters, audits, facts and Puppet
classes, is not authorized beyond requiring any view_hosts permission.

(cherry picked from commit 7a86dcfe6b36dd43cd6163ce70599e53f09cc217)

History

#1 - 07/12/2016 03:58 AM - Dominic Cleal

- Related to Bug #8343: API resource_scope ignores options added

#2 - 07/12/2016 04:00 AM - Dominic Cleal

Further details from Daniel's report:

```
I dug into this, and here's the problem:

  - https://github.com/theforeman/foreman/blob/1.12.0/app/controllers/concerns/find_common.rb#L37
    is called from:
    https://github.com/theforeman/foreman/blob/1.12.0/app/controllers/api/base_controller.rb#L302
    because we have to get the 'parent scope' (the parent scope for the
    'Interfaces' resource, is 'Host')
  - scope_for is called so we get the list of hosts, scoped by permissions
  - on line 42 we make this check 'resource.respond_to?(:authorized)',
    which is called upon Host, therefore `Host.respond_to? :authorized`.

That returns false, because Host is a module, not a class. The class
that would return true to that would be Host::Base. We're aware
of this issue and we overcome it like this
https://github.com/theforeman/foreman/blob/1.12.0/app/models/host.rb#L21

I've changed the regex to be /(\Afind_by_(.*)\Z)|(\Aauthorized\Z)/ and
that fixes the problem. Notice this check would fail for any
/api/v2/hosts/:id/WHATEVER_RESOURCE , so audits, smart_class_parameters,
reports/last, smart_variables, facts can be affected too.
```

The change seems to have been introduced by #8343, as in 1.9-stable, the controller would always use an .authorized scope to find nested objects (i.e. the host of an interfaces call): https://github.com/theforeman/foreman/blob/1.9-stable/app/controllers/api/base_controller.rb#L215-L223. Since then, it checks that the parent resource responds to .authorized, as noted above.

#3 - 07/12/2016 04:06 AM - Dominic Cleal

My suggestion for a fix is to improve the extract_resource_from_param/resource_class_for methods to return Host::Managed rather than the Host module, which means the authorisation and or methods will always be against the correct object. Changing the behaviour of Host might lead to more subtle bugs.

#4 - 07/12/2016 05:25 AM - Dominic Cleal

- Subject changed from Access to API host interfaces, parameters etc. are not restricted by view_hosts filters to CVE-2016-5390 - access to API host interfaces, parameters etc. are not restricted by view_hosts filters

#5 - 07/12/2016 02:44 PM - The Foreman Bot

- Status changed from Assigned to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/3644 added

#6 - 07/19/2016 09:02 AM - Daniel Lobato Garcia

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 7a86dcfe6b36dd43cd6163ce70599e53f09cc217.

#7 - 08/22/2016 03:18 AM - Dominic Cleal

- Related to Bug #16219: Association named 'hostgroup' was not found on Nic::Base added