Foreman - Bug #11579

CVE-2015-5233 - reports show/destroy not restricted by host authorization

08/27/2015 03:27 AM - Dominic Cleal

Status:	Closed		
Priority:	High		
Assignee:	Daniel Lobato Garcia		
Category:	Security		
Target version:	1.8.4		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.5.0
Bugzilla link:	1263741	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/2644		

Description

Foreman 1.5.0 or higher are vulnerable to an authorization issue that allows users to view and delete reports for hosts that they don't have access to.

Reports (from tools such as Puppet) are stored in Foreman and associated to the host they came from. Users can be granted permissions to view and/or destroy reports, and also separate permissions to view certain hosts. The UI and API only list reports where the user has permission to view both reports and the host it was from.

The security issue is that both the show and destroy actions for viewing and deleting individual reports do not limit access to the hosts that the user has permission to view. A user with permission to view or destroy reports can do so for any host if they know the ID, or can easily view the last report for a given host.

Thanks to Daniel Lobato Garcia of Red Hat for reporting this to foreman-security@googlegroups.com.

Associated revisions

Revision 293036df - 09/01/2015 10:51 AM - Daniel Lobato Garcia

Fixes #11579 - Reports show/destroy restricted by host authorization (CVE-2015-5233)

ReportsController 'show' and 'destroy' now perform a check to see if the User is authorized to see the Host associated with the Report. In case it's not, it returns 404, as to not give hints whether a Report ID or Host ID are valid.

I followed the same approach on the API controllers. 'last' was not vulnerable due to using my_reports which performs the necessary check on 'view_hosts' permission.

Revision d213e460 - 09/09/2015 11:37 AM - Daniel Lobato Garcia

Fixes #11579 - Reports show/destroy restricted by host authorization (CVE-2015-5233)

ReportsController 'show' and 'destroy' now perform a check to see if the User is authorized to see the Host associated with the Report. In case it's not, it returns 404, as to not give hints whether a Report ID or Host ID are valid.

I followed the same approach on the API controllers. 'last' was not vulnerable due to using my_reports which performs the necessary check on 'view_hosts' permission.

(cherry picked from commit 293036dfa71ae70624663647f1ef70798bf53d3e)

Revision be0b9bee - 09/15/2015 09:33 AM - Daniel Lobato Garcia

Fixes #11579 - Reports show/destroy restricted by host authorization (CVE-2015-5233)

ReportsController 'show' and 'destroy' now perform a check to see if the User is authorized to see the Host associated with the Report. In

case it's not, it returns 404, as to not give hints whether a Report ID or Host ID are valid.

I followed the same approach on the API controllers. 'last' was not vulnerable due to using my_reports which performs the necessary check on 'view_hosts' permission.

(cherry picked from commit 293036dfa71ae70624663647f1ef70798bf53d3e)

History

#1 - 08/27/2015 03:28 AM - Dominic Cleal

It looks like this extends to both the regular #show and #destroy behaviour on the UI and API controllers, which would allow somebody with *_reports permission but not the associated host to view or destroy a report.

I think the vulnerable locations are:

1. ReportsController#show, #destroy - allowing viewing and deletion of reports for users with the appropriate *_reports permission but not the appropriate view_hosts permission. (Not just "last".)

2. API ReportsController#show, #destroy - ditto, but I think the #last method is safe as it uses Report.my_reports.

The authorisation here is complex and two-fold, as it's both using .authorized and .my_reports to limit based on both reports **and** host permissions (inc taxonomies).

#2 - 08/27/2015 03:32 AM - Dominic Cleal

- Description updated

#3 - 08/27/2015 03:57 AM - Daniel Lobato Garcia

- Assignee set to Daniel Lobato Garcia

#4 - 08/27/2015 11:24 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/2644 added

- Pull request deleted ()

#5 - 09/01/2015 10:52 AM - Dominic Cleal

- translation missing: en.field_release changed from 72 to 84

#6 - 09/01/2015 11:01 AM - Daniel Lobato Garcia

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 293036dfa71ae70624663647f1ef70798bf53d3e.

#7 - 09/16/2015 10:52 AM - Bryan Kearney

- Bugzilla link set to 1263741