Foreman - Bug #13828

CVE-2016-2100 - unprivileged user can see private bookmarks in Administer -> Bookmarks

02/22/2016 04:28 AM - Ohad Levy

Status:	Closed		
Priority:	Normal		
Assignee:	Tom Caspy		
Category:	Security		
Target version:	1.10.3		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:	1192414	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/3221		

Description

Cloned from https://bugzilla.redhat.com/show_bug.cgi?id=1192414
Description of problem:
Unprivileged user can see Administer -> Bookmarks

How reproducible:
always

Steps to Reproduce:
1. Login with admin user
2. Switch to "Any context" and create user without any location, org and role
3. Logout with admin user and login with newly created user

Actual results:
The unprivileged user can access Administer -> Bookmarks. He can not get details about these bookmarks, details about these bookmarks, but see them.

Associated revisions

Revision a61344da - 02/29/2016 08:35 AM - Tom Caspy

fixes #13828 - CVE-2016-2100 - only showing relevant bookmarks

Revision f211de7e - 03/10/2016 10:49 AM - Tom Caspy

fixes #13828 - CVE-2016-2100 - only showing relevant bookmarks

(cherry picked from commit a61344da14f73920b4bdc7ad8220e7a0ed998031)

Revision 548f822d - 03/29/2016 02:22 PM - Tom Caspy

fixes #13828 - CVE-2016-2100 - only showing relevant bookmarks

(cherry picked from commit a61344da14f73920b4bdc7ad8220e7a0ed998031)

History

#1 - 02/22/2016 04:29 AM - Ohad Levy

I would expect bookmark listing to display my_bookmarks by default, similar to how the bookmark dropdown works.

#2 - 02/22/2016 04:30 AM - Ohad Levy

- Description updated

#3 - 02/22/2016 06:03 AM - Dominic Cleal

- Subject changed from unprivileged user can see Administer -> Bookmarks to unprivileged user can see private bookmarks in Administer -> Bookmarks

- Category set to Security

- Assignee deleted (Tom Caspy)

I think you specifically mean other user's private bookmarks are visible, so updated. The page and public bookmarks should be accessible to any user.

Please report security issues first to foreman-security, don't just file them in Redmine. See http://theforeman.org/security.html and https://groups.google.com/forum/#!msg/foreman-dev/noN-XJ1qXgU/vYFPVYLQDQAJ for more information. I will forward and start the CVE process myself.

#4 - 02/22/2016 08:03 AM - Dominic Cleal

There are further related issues with bookmarks, mostly coming from resource_base not being adequately defined:

- UI edit action can render a form for a private bookmark by ID, if the user has edit_permission.
- API index and get responses also shows private bookmarks from other users
- update and destroy actions of both the UI and API are not scoped to bookmarks that the user should have access to update, so they can supply an ID for a private bookmark of another user, the resource is found and updated. User needs edit/destroy_bookmarks permission for this.

I've requested a CVE for this issue, we'll address it in the next release(s) following a patch being written.

#5 - 02/22/2016 08:49 AM - Dominic Cleal

- Subject changed from unprivileged user can see private bookmarks in Administer -> Bookmarks to CVE-2015-7582 - unprivileged user can see private bookmarks in Administer -> Bookmarks

CVE-2015-7582 has been assigned. Please include the number in the commit message.

#6 - 02/22/2016 08:51 AM - Tom Caspy

- File Screen Shot 2016-02-22 at 3.50.23 PM.png added

tried reproducing with unpriviliged user, failed.

#7 - 02/22/2016 08:52 AM - Tom Caspy

but I can see all the hosts in the system, can't edit them. is that supposed to happen?

#8 - 02/22/2016 08:54 AM - Dominic Cleal

Depends on the permissions assigned to your "Anonymous" role, which is a minimum set applied to all users.

The default changed some time ago and view_hosts was removed. view_bookmarks is assigned by default, so ensure yours matches the default seed (db/seeds.d/03-roles.rb).

#9 - 02/22/2016 09:51 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Tom Caspy

- Pull request https://github.com/theforeman/foreman/pull/3217 added

#10 - 02/23/2016 03:08 AM - Dominic Cleal

- Subject changed from CVE-2015-7582 - unprivileged user can see private bookmarks in Administer -> Bookmarks to CVE-2016-2100 - unprivileged user can see private bookmarks in Administer -> Bookmarks

The CVE identifier should have been assigned from a 2016 block, so it's now CVE-2016-2100.

#11 - 02/23/2016 09:53 AM - Tom Caspy

- Status changed from Ready For Testing to New

- Assignee deleted (Tom Caspy)

#12 - 02/23/2016 09:54 AM - Tom Caspy

- Pull request deleted (https://github.com/theforeman/foreman/pull/3217)

#13 - 02/23/2016 10:13 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Assignee set to Tom Caspy

- Pull request https://github.com/theforeman/foreman/pull/3221 added

#14 - 02/29/2016 08:33 AM - Dominic Cleal

- translation missing: en.field_release set to 145

#15 - 02/29/2016 09:01 AM - Tom Caspy

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset a61344da14f73920b4bdc7ad8220e7a0ed998031.

Files

Screen Shot 2016-02-22 at 3.50.23 PM.png	13.7 KB	02/22/2016	Tom Caspy