Foreman - Bug #18245

Enabling OAuth is too dangerous

01/25/2017 05:47 PM - M T

Status:	New		
Priority:	Normal		
Assignee:			
Category:	Users, Roles and Permissions		
Target version:			
Difficulty:	medium	**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.13.3
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The current OAuth implementation in Foreman allows access to anybody with knowledge of two strings: OAuth consumer key and OAuth consumer secret.

In this sense, it is not any more secure than the typical username/password set of credentials.

But, in reality, it is **a lot worse**:

1. Unlike personal passwords, which are never shown in clear text, both the key and the secret are visible to all current admins under FOREMAN/settings#Auth
2. While personal passwords can be made to automatically expire (such as by using an external LDAP-server with stricter settings), the OAuth credentials are permanent
3. If mapping of OAuth-requests to existing accounts is not enabled, using this method gives the REST API scripts *admin*-level access to Foreman -- having once observed the credentials, a hacker can delete or alter hosts in Foreman.
4. If mapping of OAuth-requests to existing accounts is enabled (by specifying a separete request-header FOREMAN-USER), a script can freely impersonate *any* user -- which is even worse than anonymous admin-access. Once authenticated with the OAuth credentials, a script can gain any user's authorization...

The existing OAuth implementation should be redone to:

- Allow only read-only access to OAuth-using scripts by default, if OAuth is enabled at all.
- Allow admins to create multiple OAuth credential-pairs with different roles, limiting the capabilities of API-using scripts

Finally, OAuth or not, there should be a way to enable *anonymous* browsing/searching of Foreman data -- even if making any changes may still require a login. The current :login: true in settings.yaml is not granular enough.

Related issues:

Related to Foreman - Feature #1301: Consider adding a per-user API key	**Closed**

History

#1 - 01/26/2017 02:57 AM - Dominic Cleal

- Related to Feature #1301: Consider adding a per-user API key added