Foreman - Bug #5463

No authentication required for /unattended/provision?hostname=HOSTNAME

04/26/2014 12:44 AM - Dylan Charleston

Status:	Duplicate		
Priority:	Normal		
Assignee:			
Category:	Security		
Target version:			
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	1.4.0
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

I'm finding that there is no authentication needed when viewing https://foreman-server/unattended/provision?hostname=HOSTNAME and I see the same behavior on finish/pxelinux/etc.

I have ":login: true" in the foreman settings.yml file and user accounts are setup to authenticate through LDAP. Looking at debug logs on the Foreman server, I see the following:

When requesting the /unattended/provision file -

Started GET "/unattended/provision?hostname=some.host.name" for 10.10.10.112 at 2014-04-25 13:51:47 -0700
Processing by UnattendedController#provision as HTML
Parameters: {"hostname"=>"some.host.name"}
Host::Managed Load (2.3ms) SELECT `hosts`.* FROM `hosts` WHERE `hosts`.`type` IN ('Host::Managed') AND `hosts`.`ip` IS NULL LIMIT 1
Host::Managed Load (1.3ms) SELECT `hosts`.* FROM `hosts` WHERE `hosts`.`type` IN ('Host::Managed') AND `hosts`.`name` = 'some.host.name' LIMIT 1
Operatingsystem Load (3.9ms) SELECT `operatingsystems`.* FROM `operatingsystems` WHERE `operatingsystems`.`id` = 2 ORDER BY operatingsystems.name LIMIT 1
Found some.host.name
Medium Load (1.0ms) SELECT `media`.* FROM `media` WHERE `media`.`id` = 7 ORDER BY media.name LIMIT 1
Architecture Load (0.9ms) SELECT `architectures`.* FROM `architectures` WHERE `architectures`.`id` = 1 LIMIT 1
ConfigTemplate Load (3.9ms) SELECT `config_templates`.* FROM `config_templates` INNER JOIN `config_templates_operatingsystems` ON `config_templates_operatingsystems`.`config_template_id` = `config_templates`.`id` INNER JOIN `operatingsystems` ON `operatingsystems`.`id` = `config_templates_operatingsystems`.`operatingsystem_id` INNER JOIN `template_kinds` ON `template_kinds`.`id` = `config_templates`.`template_kind_id` INNER JOIN `template_combinations` ON `template_combinations`.`config_template_id` = `config_templates`.`id` INNER JOIN `environments` ON `environments`.`id` = `template_combinations`.`environment_id` WHERE `operatingsystems`.`id` = 2 AND `template_kinds`.`name` = 'provision' AND `environments`.`id` = 8 ORDER BY config_templates.name LIMIT 1
ConfigTemplate Load (2.1ms) SELECT `config_templates`.* FROM `config_templates` INNER JOIN `config_templates_operatingsystems` ON `config_templates_operatingsystems`.`config_template_id` = `config_templates`.`id` INNER JOIN `operatingsystems` ON `operatingsystems`.`id` = `config_templates_operatingsystems`.`operatingsystem_id` INNER JOIN `template_kinds` ON `template_kinds`.`id` = `config_templates`.`template_kind_id` INNER JOIN `os_default_templates` ON `os_default_templates`.`config_template_id` = `config_templates`.`id` WHERE `operatingsystems`.`id` = 2 AND `template_kinds`.`name` = 'provision' AND `os_default_templates`.`operatingsystem_id` = 2 ORDER BY config_templates.name LIMIT 1
rendering DB template Preseed Ubuntu - provision
ComputeResource Load (1.0ms) SELECT `compute_resources`.* FROM `compute_resources` WHERE `compute_resources`.`id` = 1 ORDER BY compute_resources.name LIMIT 1
Subnet Load (1.1ms) SELECT `subnets`.* FROM `subnets` WHERE `subnets`.`id` = 3 ORDER BY vlanid LIMIT 1
Domain Load (0.9ms) SELECT `domains`.* FROM `domains` WHERE `domains`.`id` = 1 ORDER BY domains.name LIMIT 1
Ptable Load (1.2ms) SELECT `ptables`.* FROM `ptables` WHERE `ptables`.`id` = 2 ORDER BY ptables.name LIMIT 1
CommonParameter Load (1.0ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('CommonParameter') ORDER BY parameters.name
Organization Load (0.9ms) SELECT `taxonomies`.* FROM `taxonomies` WHERE `taxonomies`.`type` IN ('Organization') AND `taxonomies`.`id` = 18 LIMIT 1
OrganizationParameter Load (1.1ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('OrganizationParameter') AND `parameters`.`reference_id` = 18 ORDER BY parameters.name

Location Load (0.8ms) SELECT `taxonomies`.* FROM `taxonomies` WHERE `taxonomies`.`type` IN ('Location') AND `taxonomies`.`id` = 1 LIMIT 1
LocationParameter Load (0.9ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('LocationParameter') AND `parameters`.`reference_id` = 1 ORDER BY parameters.name
DomainParameter Load (1.1ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('DomainParameter') AND `parameters`.`reference_id` = 1 ORDER BY parameters.name
OsParameter Load (0.9ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('OsParameter') AND `parameters`.`reference_id` = 2 ORDER BY parameters.name
HostParameter Load (1.0ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('HostParameter') AND `parameters`.`reference_id` = 767 ORDER BY parameters.name
(0.8ms) SELECT puppetclass_id FROM `host_classes` WHERE `host_classes`.`host_id` = 767
LookupKey Load (0.6ms) SELECT `lookup_keys`.* FROM `lookup_keys` WHERE `lookup_keys`.`puppetclass_id` IN (NULL) ORDER BY lookup_keys.key
CACHE (0.0ms) SELECT `parameters`.* FROM `parameters` WHERE `parameters`.`type` IN ('CommonParameter') ORDER BY parameters.name
CACHE (0.0ms) SELECT puppetclass_id FROM `host_classes` WHERE `host_classes`.`host_id` = 767
CACHE (0.0ms) SELECT `lookup_keys`.* FROM `lookup_keys` WHERE `lookup_keys`.`puppetclass_id` IN (NULL) ORDER BY lookup_keys.key
Token Load (1.1ms) SELECT `tokens`.* FROM `tokens` WHERE `tokens`.`host_id` = 767 LIMIT 1
Rendered inline template (57.4ms)
Completed 200 OK in 92ms (Views: 43.9ms | ActiveRecord: 29.9ms)

Other page functioning normal:

Started PUT "/settings/46" for 10.10.10.112 at 2014-04-25 13:48:27 ~~0700~~
~~Processing by SettingsController#update as JSON~~
~~Parameters: {"setting"=>{"value"=>"[FILTERED]"}, "id"=>"46",~~
~~"authenticity_token"=>""Hq3JajlWLQWOCOgpxGF+BGXKCIlijlijjkQUNiTYWFI=""}~~
~~User Load (1.8ms) SELECT `users`.* FROM `users` WHERE `users`.`id` = 2 LIMIT 1~~
~~Setting current user thread-local variable to someuser~~
~~(0.7ms) SELECT COUNT(~~**~~) FROM `taxonomies` WHERE `taxonomies`.`type` IN ('Organization')~~**
~~Setting current organization thread-local variable to none~~
~~(0.6ms) SELECT COUNT(~~~~) FROM `taxonomies` WHERE `taxonomies`.`type` IN ('Location')~~
~~Setting current location thread-local variable to none~~
~~(1.0ms) SELECT id FROM `taxonomies` WHERE `taxonomies`.`type` IN ('Location') LIMIT 1~~
~~(0.6ms) SELECT id FROM `taxonomies` WHERE `taxonomies`.`type` IN ('Organization') LIMIT 1~~
~~Setting Load (1.1ms) SELECT `settings`.* FROM `settings` WHERE `settings`.`id` = 46 ORDER BY name LIMIT 1~~
~~(0.4ms) BEGIN~~
~~Setting Exists (0.7ms) SELECT 1 AS one FROM `settings` WHERE (`settings`.`name` = BINARY 'token_duration' AND `settings`.`id` != 46) LIMIT 1~~
~~removing token_duration from cache~~
~~CACHE (0.0ms) SELECT `settings`.* FROM `settings` WHERE `settings`.`id` = 46 ORDER BY name LIMIT 1~~
~~(0.8ms) SELECT MAX AS max_id FROM `audits` WHERE `audits`.`auditable_id` = 46 AND `audits`.`auditable_type` = 'Setting'~~
~~SQL (0.7ms) INSERT INTO `audits` (`action`, `associated_id`, `associated_name`, `associated_type`, `auditable_id`, `auditable_name`, `auditable_type`, `audited_changes`, `comment`, `created_at`, `remote_address`, `user_id`, `user_type`, `username`, `version`) VALUES ('update', NULL, NULL, NULL, 46, 'token_duration', 'Setting', '~~\nvalue:\n- ! \'--- 0\n\n ...\n\n\'\n- \n', NULL, '2014-04-25 20:48:27', '10.10.10.112', NULL, NULL, 'Some User', 2)
(0.9ms) UPDATE `settings` SET `value` = NULL, `updated_at` = '2014-04-25 20:48:27' WHERE `settings`.`category` IN ('Setting::Provisioning') AND `settings`.`id` = 46
(9.6ms) COMMIT
Completed 200 OK in 52ms (Views: 2.7ms | ActiveRecord: 18.8ms)

It seems like it just skips the "Setting current user thread-local variable to someuser" line for the /unattended/provision page. /unattended/provision?spoof=HOSTNAME requires auth so it seems like this is just a bug.

Related issues:

Is duplicate of Foreman - Bug #5436: CVE-2014-0192 - provisioning templates a...	**Closed**	**04/24/2014**

History

#1 - 04/28/2014 08:03 AM - Dominic Cleal

- Is duplicate of Bug #5436: CVE-2014-0192 - provisioning templates are world accessible added

#2 - 04/28/2014 08:04 AM - Dominic Cleal

- Status changed from New to Duplicate

Thanks for the report, closing as a dupe of #5436.