Foreman - Bug #2121

Unauthenticated YAML fact and reports importers can be exploited

01/09/2013 11:58 AM - Dominic Cleal

Status:	Closed		
Priority:	Immediate		
Assignee:	Dominic Cleal		
Category:	Security		
Target version:	1.1		
Difficulty:		**Fixed in Releases:**	
Triaged:		**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:			

Description

The Rails vulnerability CVE-2013-0156 has made us realise there's a very similar issue in Foreman itself where it parses untrusted YAML input.

The facts and reports importers are used by puppetmasters to send YAML to Foreman, which is imported straight from Puppet and without any
authentication (since the puppetmaster has no credentials). An attacker can use this YAML loading to exploit Foreman.

We're proposing to lock this down so that only hosts with registered smart proxies on (with the Puppet feature) are able to upload data.

In addition, we would recommend (and implement in foreman-installer) enabling optional client SSL cert verification in mod_ssl, then enforce
the smart proxy check using the client certificate's CN. The report and ENC scripts would change to use the puppetmaster's SSL cert during HTTPS calls to Foreman.

Both the host check and the enhanced HTTPS check would have settings so they can be disabled. They'd be enabled by default in 1.1, but if
there's demand for a backport to 1.0 then they'd be disabled for compatibility.

This would also address the issue raised by Andreas Rogge (thank you for the report) where ENC output, including hashed root passwords, is
accessible to any host: #2069

In the meantime, if you're concerned about the security of your Foreman host then you could restrict access via Apache, if you use it. e.g.

```
<Location ~ "/(fact_values|reports)/create">
  Order Deny,Allow
  Deny from all
  Allow from puppetmaster.example.net
</Location>
```

(from http://groups.google.com/group/foreman-users/browse_thread/thread/fe39ca595e1f03db)

Related issues:

Related to Foreman - Bug #2069: (encrypted) root passwords are world readable	**Closed**	**10/07/2009**
Related to Foreman - Bug #2151: Issues with SSL verification of proxies	**Closed**	**01/22/2013**
Related to Foreman - Feature #2153: Add trusted_hosts for puppetmaster interf...	**Closed**	**01/24/2013**
Related to Foreman - Feature #5914: Allow a host to upload its own facts and ...	**New**	**05/23/2014**

Associated revisions

Revision 358ec5a3 - 01/20/2013 10:06 AM - Dominic Cleal

fixes #2121, #2069 - restrict importers and ENC to puppetmasters and users

CVE-2013-0171: report and fact importers parse YAML directly from the remote host without authentication. Untrusted YAML can instantiate objects and be used to exploit Foreman.

CVE-2013-0174: external nodes (ENC) output is available to any source and could contain sensitive information, e.g. root password.

The restrict_registered_puppetmasters setting (default: on) now only permits access to the three routes if the remote host has a smart proxy registered with the Puppet feature.

The require_ssl_puppetmasters setting (default: on) requires a client SSL certificate on HTTPS requests. The CN is checked against known smart proxies as above. :require_ssl in settings.yaml is recommended to disable HTTP.

Ensure ENC (node.rb) and report (foreman.rb) scripts are updated to supply client SSL certificates.

Revision 7697116c - 01/23/2013 10:26 AM - Dominic Cleal

fixes #2121, #2069 - authenticate to Foreman with SSL certificate

CVE-2013-0171 and CVE-2013-0174 were resolved by verifying client SSL certificates on Foreman interfaces used by puppetmasters. This change updates the ENC and report processors to provide and verify certificates by default.

Revision 0e3c84fc - 01/23/2013 11:11 AM - Dominic Cleal

refs #2121 - document SSL usage and configuration

Revision 0c3307cd - 01/24/2013 02:14 PM - Dominic Cleal

refs #2121 - document SSL usage and configuration

History

#1 - 01/10/2013 07:53 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

#2 - 01/15/2013 07:20 AM - Dominic Cleal

- Status changed from Assigned to Ready For Testing

Two PRs submitted:

https://github.com/theforeman/foreman/pull/373 restricts access to the puppetmaster interfaces to prevent unauthed imports (CVE-2013-0171)
https://github.com/theforeman/puppet-foreman/pull/34 to support restricted access

(linked to #2069)

#3 - 01/20/2013 10:55 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 358ec5a3a1b59c098b5c14fcd7a90ca1a6a5dccd.

#4 - 02/07/2013 03:03 AM - Dominic Cleal

For users updating and hitting this change, please see the following documentation:

- Release notes: Authentication for puppetmasters
- Manual: Securing Communications with SSL

We appreciate it's a difficult change, but is necessary to improve the security of the application. If you have problems, do check the troubleshooting text in the manual, and do contact one of the Support channels.

#5 - 05/27/2014 08:14 AM - Dominic Cleal

- Related to Feature #5914: Allow a host to upload its own facts and reports - Support masterless Puppet added