Foreman - Bug #2069

(encrypted) root passwords are world readable

12/21/2012 05:05 AM - Andreas Rogge

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

Description

This is related to #39.
Essentially I do ask for the same feature, but I believe it is not a feature request, but a major security issue.

Right now anyone can download the external nodes YAML without any limitation. For a really basic setup (that doesn't even use external nodes) it looks like this:

--
parameters:
puppetmaster: puppet.master.server.fqdn
owner_email: owner@domain.tld
foreman_env: &id001 production
owner_name: Admin User
root_pw: $1$GDJmRQFN$3hXafZx7hyZdbaL5q2Q8t1
classes: []

As you can see this makes the hash of the root password world readable.

The access to the external nodes script should be limited.
Maybe simply by checking the remote ip address against an array of configured addresses. We definitely need to set the default to no access.

We did move the password hashes from /etc/passwd to /etc/shadow in the early nineties by intent: they should not be world-readable.

Related issues:

Related to Foreman - Bug #2121: Unauthenticated YAML fact and reports importe...	**Closed**	**01/09/2013**
Related to Foreman - Feature #2127: Support newer hash schemes for root passw...	**Closed**	**01/15/2013**
Related to Foreman - Bug #3060: Remove YAML host permissions from basic users,	**New**	**09/09/2013**

Associated revisions

Revision 31b7d5de - 01/15/2013 10:59 AM - Dominic Cleal

fixes #2069 - use a random salt when saving the root password

CVE-2013-0173: insecure fixed salt "foreman" for passwords

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 24de57c0 - 01/20/2013 10:20 AM - Dominic Cleal

refs #2069 - enable auth by default

Without authentication, sensitive information and power is available to all,
so improve security out of the box.

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 c29484db - 01/23/2013 10:26 AM - Dominic Cleal

refs #2069 - enable auth by default

Without authentication, sensitive information and power is available to all,
so improve security out of the box.

History

#1 - 12/21/2012 12:57 PM - Sam Kottler

- Category changed from External Nodes to Security

- Assignee deleted (Ohad Levy)

- Priority changed from High to Normal

I agree this would be a nice to have, but it's not a security risk if you're ensuring that your systems don't use MD5 (and maybe not SHA-1). Even using SHA-1 is relatively safe, though because a lot of effort is required to break it. If you use a 6 character password (too short IMO) it takes there are 6.236738252 × 10^{35} permutations; it would take roughly 8.909626074×10^{26} CPU years to crack it at 700,000,000 tries a second.

Also, this can be mitigated easily with iptables/firewalld/SG's. @Ohad Levy - what do you think?

#2 - 12/21/2012 01:04 PM - Greg Sutcliffe

Personally I mitigate this by blocking root access via SSH+password as part of my initial puppet run (which I do during the installer).

However, it is something we should fix at some point. Perhaps we should add a Setting (default to Off) which is an array of IPs which are allowed to recieve externalnodes?

#3 - 12/21/2012 01:14 PM - Ohad Levy

or maybe have a setting that only allow ip's from smart proxies with puppet feature?

#4 - 12/22/2012 01:52 PM - Andreas Rogge

I see two issues here:

1. The default configuration is insecure
All products should be shipped with secure defaults. This is not the case with foreman currently.
I also don't think that recent hashing algorithms work around the problem sufficiently, because by default foreman ships with a well known default password hash.
Whatever you say: this is not what I'd call secure by default.

2. There is no simple/obvious way to deny access to the YML
I googled the topic and there was no documentation available on how to limit access.
Also I haven't found a simple way to deny access. The Information is available through at least two different URLs, so URL pattern matching is probably not sufficient - I cannot be sure there isn't another URL I need to block.

Even if we choose to ship insecure by default, there should be a simple way to make this part of the system more secure.

#5 - 01/09/2013 11:58 AM - Dominic Cleal

- Priority changed from Normal to High

- Target version set to 1.1

- Difficulty changed from easy to medium

Proposal above of limiting access to smart proxy hosts by default has been posted here and in #2121:
http://groups.google.com/group/foreman-users/browse_thread/thread/fe39ca595e1f03db

In addition, we're looking to verify the SSL certs to ensure it's just the puppet process on the system that has access.

#6 - 01/10/2013 07:54 AM - Dominic Cleal

- Status changed from New to Assigned

- Assignee set to Dominic Cleal

#7 - 01/15/2013 07:19 AM - Dominic Cleal

- Status changed from Assigned to Ready For Testing

Some PRs submitted:

https://github.com/theforeman/foreman/pull/372 fixes password hashing (CVE-2013-0173)
https://github.com/theforeman/foreman/pull/373 restricts access to the ENC interface (CVE-2013-0174)
https://github.com/theforeman/puppet-foreman/pull/34 to support restricted access and enable login by default

I'd like to go further in restricting the viewing of hashes to authenticated users too, obfuscating them in ENC, host edit, settings and template previews, but that work isn't complete.

#8 - 01/15/2013 11:21 AM - Dominic Cleal

- Status changed from Ready For Testing to Closed

- % Done changed from 0 to 100

Applied in changeset 31b7d5de00c21735164fa92940e6be2c08820c37.

#9 - 01/15/2013 11:37 AM - Dominic Cleal

- Status changed from Closed to Ready For Testing

- % Done changed from 100 to 50

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

- Status changed from Ready For Testing to Closed

- % Done changed from 50 to 100

Applied in changeset 358ec5a3a1b59c098b5c14fcd7a90ca1a6a5dccd.

#11 - 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.

#12 - 09/09/2013 05:19 PM - Dominic Cleal

- Related to Bug #3060: Remove YAML host permissions from basic users, added