Installer - Bug #30489

CVE-2020-14335 world-readable OMAPI secret

07/24/2020 09:55 PM - Ondřej Ezr

Status:	Closed		
Priority:	Normal		
Assignee:	Ondřej Ezr		
Category:	Foreman modules		
Target version:	2.1.3		
Difficulty:	medium	**Fixed in Releases:**	2.1.3, 2.2.0
Triaged:	Yes	**Found in Releases:**	
Bugzilla link:	1858311	**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/puppet-foreman_proxy/pull/614, https://github.com/theforeman/puppet-foreman_proxy/pull/615, https://github.com/theforeman/foreman-installer/pull/576		

Description

Related issues:

Related to Installer - Bug #30973: Fix for CVE-2020-14335 cause breakage on 2...	**Duplicate**

Associated revisions

Revision 7ca431f4 - 09/22/2020 03:57 PM - Ondřej Ezr

Fixes #30489 - CVE-2020-14335 world-readable OMAPI

Revision 60891601 - 09/23/2020 11:44 AM - Ondřej Ezr

Refs #30489 - enable dhcp acls by default

Both puppet-dhcp and puppet-foreman_proxy are ready to handle acls on both supported systems.
The best approach here is to leverage this to our favor instead of enforcing a user or mode on config files.

History

#1 - 07/24/2020 10:49 PM - Ondřej Ezr

- File 0001-BZ-1858311-CVE-2020-14335-dhcpd.conf-permissions.patch added

Adding a proposed patch

#2 - 07/28/2020 07:36 AM - Tomer Brisker

- Bugzilla link set to 1858311

#3 - 07/28/2020 09:26 AM - Ewoud Kohl van Wijngaarden

Are you sure this works? It looks like it disables omapi unless a key and secret are set. This is something that the proxy actually needs to make modifications. To verify, you should create/modify/delete a DHCP reservation via the Smart Proxy API.

It also breaks on Debian where we don't set ACLs and Smart Proxy needs to read the config files to determine the hardcoded leases.

I also don't like the modification of file permissions from another module because it feels very unreliable. This may make a cherry pick easier so I'd be OK with that just for the picks. For upstream we should really modify puppet-dhcp as well. For example, expose the directory mode. Then I'd also be OK with a breaking change that makes it secure by default.

Going forward I'd suggest we write up a minimal verification script that checks DHCP works. Currently we have no such verification.

#4 - 07/28/2020 10:55 AM - Ewoud Kohl van Wijngaarden

Setting the mode on /etc/dhcp/dhcpd.conf to 640 breaks things because we don't set an ACL in that - only the directory itself. This can be seen in the

Smart Proxy log:

```
Jul 28 10:43:09 centos7-katello-nightly.wisse.example.com smart-proxy[7201]: /usr/share/foreman-proxy/modules/dhcp_isc/isc_state_changes_observer.rb:170:in `read': Permission denied @ rb_sysopen - /etc/dhcp/dhcpd.conf (Errno::EACCES)
```

You can then see that the API returns no subnets anymore:

```
# curl -s --cert /etc/foreman-proxy/foreman_ssl_cert.pem --key /etc/foreman-proxy/foreman_ssl_key.pem https://$HOSTNAME:9090/dhcp | jq
[]
```

Compare this to what it returned prior to the change:

```
# curl -s --cert /etc/foreman-proxy/foreman_ssl_cert.pem --key /etc/foreman-proxy/foreman_ssl_key.pem https://$HOSTNAME:9090/dhcp | jq
[
  {
    "network": "192.168.122.0",
    "netmask": "255.255.255.0",
    "options": {}
  }
]
```

And for the record, to create a reservation, you can use this:

```
curl -s --cert /etc/foreman-proxy/foreman_ssl_cert.pem --key /etc/foreman-proxy/foreman_ssl_key.pem https://$HOSTNAME:9090/dhcp/192.168.122.0 -X POST -d ip=192.168.122.100 -d mac=00:00:00:ff:ff:ff -d hostname=host.example.com
```

Then list it:

```
# curl -s --cert /etc/foreman-proxy/foreman_ssl_cert.pem --key /etc/foreman-proxy/foreman_ssl_key.pem https://$HOSTNAME:9090/dhcp/192.168.122.0 | jq
```

See https://projects.theforeman.org/projects/smart-proxy/wiki/API as well.

Also note that by default the DHCP package sets the mode of /etc/dhcp/dhcpd.conf to 644 so that should be safe - the directory is sufficient.

What should also be done is to create an omapi key by default, otherwise you can still access port 7911 without auth and setting the directory mode is useless.

#5 - 07/29/2020 11:55 AM - Ondřej Ezr

You are right, not enabling the omapi at all is stupid.

I do not believe enforcing the key should be part of this threat though.

If you don't set a key, you may have other means to secure the port from unauthorized access. You haven't sacured it by choice.
This is about the key exposure, so about the situations, when you consider the port to be your weakpoint and you want to secure it.

I agree this should be just for cherry-picks and once we lift the embargo, I'm going to send a PR to the puppet-dhcp.

#6 - 07/30/2020 02:10 PM - Ewoud Kohl van Wijngaarden

- Target version changed from 2.2.0 to 2.1.1

#7 - 08/03/2020 01:28 PM - Ewoud Kohl van Wijngaarden

- Target version changed from 2.1.1 to 2.2.0

2.1.1 is going out and since there's still some issues, aligning to 2.2.0 again.

#8 - 08/05/2020 09:43 AM - Ondřej Ezr

- File 0002-CVE-2020-14335-dhcpd.conf-permissions.patch added

Given we won't consider the missing key as part of this vulnerability, the fix should be just changing permissions on the folder.

#9 - 08/05/2020 09:50 AM - Ondřej Ezr

- File 0003-CVE-2020-14335-dhcpd.conf-permissions.patch added

#10 - 08/05/2020 12:00 PM - Ewoud Kohl van Wijngaarden

I have pretty much no experience with overriding attributes this way so I don't know how reliable it is. Normally my approach would be to add parameters to puppet-dhcp (which is another module we do control). It makes for a more complicated cherry pick (since you need to patch two modules), but it is more straight forward in reasoning about the code. There is also no chance of a mismatch in filenames, though that could also be mitigated by using $dhcp::dhcp_dir instead of hardcoding /etc/dhcp.

Also wondering if applying ACLs on Debian is better than setting the directory group (note you missed a $ in the patch). The reason we set ACLs on Red Hat is that the DHCP package enforces a directory mode of 0750 so a yum update reverted the installer changes. I'd check for similar behavior on Debian.

#11 - 08/05/2020 03:32 PM - Ondřej Ezr

- File 0004-CVE-2020-14335-dhcpd.conf-permissions.patch added

It was just a pitch :)
I've finished that idea, with the dhcp_dir variable you have proposed.
I've tested it on debian and centos - it works on both.

I really belive we should do it in puppet-foreman_proxy module, as it's module we control, right?

I'll send patch to puppet-dhcp righ after we lift the embargo.

#12 - 08/05/2020 03:48 PM - Ewoud Kohl van Wijngaarden

Well, we maintain both modules. It might be good to have two versions: the simple to cherry pick and the proper upstream fix.

#13 - 08/06/2020 03:10 PM - Ondřej Ezr

- File 0001-CVE-2020-14335-puppet-dhcp.patch added

#14 - 08/07/2020 08:46 AM - Ondřej Ezr

- File deleted (0001-CVE-2020-14335-puppet-dhcp.patch)

#15 - 08/07/2020 03:51 PM - Ondřej Ezr

Solution should be https://github.com/theforeman/puppet-dhcp/pull/177
and once accepted use this to do what patch 0004 is doing through those parameters.

#16 - 09/07/2020 03:28 PM - Tomer Brisker

- Private changed from Yes to No

#17 - 09/08/2020 07:41 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/puppet-foreman_proxy/pull/614 added

#18 - 09/08/2020 07:51 AM - The Foreman Bot

- Pull request https://github.com/theforeman/puppet-foreman_proxy/pull/615 added

#19 - 09/10/2020 10:45 AM - The Foreman Bot

- Pull request https://github.com/theforeman/foreman-installer/pull/576 added

#20 - 09/15/2020 02:53 PM - Tomer Brisker

- Target version changed from 2.2.0 to 2.1.3

#21 - 09/22/2020 03:57 PM - The Foreman Bot

- Fixed in Releases 2.3.0 added

#22 - 09/22/2020 04:01 PM - Ondřej Ezr

- Status changed from Ready For Testing to Closed

Applied in changeset puppet-foreman_proxy|7ca431f48c39d90ad7a3fcf24a8912927e44e300.

#23 - 09/24/2020 03:11 PM - Tomer Brisker

- Fixed in Releases 2.1.3, 2.2.0 added

- Fixed in Releases deleted (2.3.0)

#24 - 10/05/2020 11:02 AM - Tomer Brisker

- Related to Bug #30973: Fix for CVE-2020-14335 cause breakage on 2.1.3 added

#25 - 10/19/2020 02:23 PM - Tomer Brisker

- Category changed from External modules to Foreman modules

Files

0001-BZ-1858311-CVE-2020-14335-dhcpd.conf-permissions.patch	1.08 KB	07/24/2020	Ondřej Ezr
0002-CVE-2020-14335-dhcpd.conf-permissions.patch	717 Bytes	08/05/2020	Ondřej Ezr
0003-CVE-2020-14335-dhcpd.conf-permissions.patch	878 Bytes	08/05/2020	Ondřej Ezr
0004-CVE-2020-14335-dhcpd.conf-permissions.patch	1.17 KB	08/05/2020	Ondřej Ezr