Packages - Privacy Issue #1092

NetworkManager 1.4 leaks hostname

2016-09-01 12:17 PM - ralessi

Status:	info needed	**% Done:**	0%
Priority:	privacy issue		
Assignee:	Megver83		
Category:			

Description

NetworkManager now uses systemd-hostnamed to get the hostname and is configured to automatically send it to any dhcp server. There is no easy way to prevent the hostname from being sent which is a privacy issue.

So far, the only way I have found is first to change the hostname, then establish the connection, then edit the connection settings and add "dhcp-send-hostname=false" to the [ipv4] block. Once this is done, one can revert to the original hostname.

History

#1 - 2016-09-26 12:39 PM - Anonymous

- Assignee set to Anonymous

#2 - 2016-12-10 03:03 PM - g4jc

This would need testing, but can probably be done.

1) Modify /etc/NetworkManager/NetworkManager.conf in networkmanager-nonprism PKGBUILD

2) Create a post-install hook that modifies users existing connections (note this will break networkmanager should they revert from nonprism)

nmcli -t -f uuid connection | while read uuid; do
nmcli connection modify $uuid \
ipv4.dhcp-send-hostname false \
ipv6.dhcp-send-hostname false
done

Code tips courtesy http://viliampucik.blogspot.com/2016/09/networkmanager-disable-sending-hostname.html

---

The potentially larger issue however is other programs which use the hostname, and logs that use the hostname.

Is disabling the hostname for one program actually helping privacy, or should we consider adding a hostname randomizer to nonprism? That way each time the computer starts the user is given a random hostname rather than the default.

#3 - 2017-01-06 02:22 AM - g4jc

Unfortunately, it is no longer possible to control the hostname from NetworkManager.

https://developer.gnome.org/NetworkManager/stable/NetworkManager.conf.html

hostname
This key is deprecated and has no effect since the hostname is now stored in /etc/hostname or other system configuration files according to build options.

This would have to be done at the dhcp client level, unfortunately there are various dhcp clients.
Additionally dispatcher.d scripts cannot be used since the pre-up scripts do not run reliably (known bug)

So that most likely leaves randomization at the systemd level.

#4 - 2017-01-07 12:54 AM - Anonymous

- Assignee changed from Anonymous to g4jc

#5 - 2017-01-09 06:10 PM - ralessi

Would it not be possible to have this line:

```
dhcp-send-hostname=false
```

automatically inserted into every new system-connection just below the [ipv4] section *before* the connection itself be activated?

With this feature working in conjunction with the mac-address randomization features that are currently working well, we should have a 'respect-your-privacy' compliant nm (at least in my opinion).

#6 - 2017-01-10 02:19 AM - g4jc

ralessi wrote:

> Would it not be possible to have this line:
> [...]
> automatically inserted into every new system-connection just below the [ipv4] section *before* the connection itself be activated?
>
> With this feature working in conjunction with the mac-address randomization features that are currently working well, we should have a 'respect-your-privacy' compliant nm (at least in my opinion).

I would be happy to implement this, but unfortunately the feature hasn't been working since at least 2014[1], and does not take into account ipv6.
So far I have only been able to get it to work with a systemd unit which replaces dhcp=internal in /etc/NetworkManager.conf with dhclient and wipes hostname on start... but even this method still leaks regularly due to race conditions on startup.

If anyone can come up with a working solution for this that does not leak hostname please let me know!

[1] http://gnome-networkmanager.2324886.n4.nabble.com/dhclient-avoiding-hostname-disclosure-via-DHCP-request-td23165.html

#7 - 2017-01-10 09:58 AM - ralessi

g4jc wrote:

> I would be happy to implement this, but unfortunately the feature hasn't been working since at least 2014[1], and does not take into account ipv6.
> So far I have only been able to get it to work with a systemd unit which replaces dhcp=internal in /etc/NetworkManager.conf with dhclient and wipes hostname on start... but even this method still leaks regularly due to race conditions on startup.

I get it. This is sinister.
Meanwhile, wouldn't it be nice to have a hostname randomizer in nonprism? And do you know how Tails deals with this issue?

#8 - 2017-01-10 12:45 PM - g4jc

ralessi wrote:

> I get it. This is sinister.
> Meanwhile, wouldn't it be nice to have a hostname randomizer in nonprism? And do you know how Tails deals with this issue?

There is preliminary work in nonprism to do this (blank and optionally randomize), but it needs to work regardless of dhcpclient. That involves race conditions. You can see the attempt I made here:
https://git.parabola.nu/abslibre.git/tree/nonprism/hostname-blanker

It doesn't work as it should. I'm not sure how Tails is dealing with it, in the past they used the now deprecated [keyfile] [hostname] of NetworkManager. If you are able to help find relevant code it could be helpful for us.

#9 - 2017-01-10 07:13 PM - ralessi

g4jc wrote:

> You can see the attempt I made here:
> https://git.parabola.nu/abslibre.git/tree/nonprism/hostname-blanker

Thanks. I'll look into this.

> It doesn't work as it should. I'm not sure how Tails is dealing with it, in the past they used the now deprecated [keyfile] [hostname] of NetworkManager. If you are able to help find relevant code it could be helpful for us.

I came across this page: https://tails.boum.org/contribute/design/#index50h3 which indicates that either the documentation or the version of nm currently used is outdated. I'll install the latest Tails and will report here what I can find.

#10 - 2017-01-12 10:21 AM - ralessi

g4jc wrote:

> I'm not sure how Tails is dealing with it, in the past they used the now deprecated [keyfile] [hostname] of NetworkManager. If you are able to help find relevant code it could be helpful for us.

I had a look at the latest Tails: they still use NetworkManager v0.9.10.0-7 and so the keyfile plugin. Considering this particular issue that seems a wise decision even though it does not comply with the 'rolling-release' concept of Parabola.

#11 - 2017-01-12 01:16 PM - ralessi

g4jc wrote:

> https://git.parabola.nu/abslibre.git/tree/nonprism/hostname-blanker

If I understand well, this script replaces the hostname that has been set permanently, but without having to reboot the system. The drawback is that the user must give up the hostname he chose to save his privacy. I am right?
For the time being, I made this very primitive script:

```
#!/bin/bash
# blank-hostname

if [ "$(id -u)" != "0" ]; then
    echo "Sorry, you are not root."
    exit 1
fi

set -e

case "$1" in
    on)
    mv /etc/hostname /etc/hostname-out
    systemctl reboot
    ;;
    off)
    mv /etc/hostname-out /etc/hostname
    systemctl reboot
    ;;
    status)
    ls /etc/hostname*
    exit
    ;;
    *)
    echo "usage blank-hostname on | off | status"
    ;;
esac
```

When I need to establish a new connection, I first do sudo blank-hostname on. Then, before doing sudo blank-hostname off, I take care of editing the connection settings with nmcli to have dhcp-send-hostname=false inserted below both of the [ipv4] and [ipv6] blocks.

#12 - 2017-02-04 05:38 PM - ralessi

This just came to me: Since networkmanager now manages the hostname via systemd-hostnamed, do you think that replacing systemd by openrc would solve this issue?

#13 - 2017-03-15 02:04 AM - g4jc

ralessi wrote:

> This just came to me: Since networkmanager now manages the hostname via systemd-hostnamed, do you think that replacing systemd by openrc would solve this issue?

I'm not sure, since I do not use OpenRC, but it may be worth testing.

Meanwhile upstream is aware of the issue and it's affect on Tails: https://bugzilla.gnome.org/show_bug.cgi?id=768076

#14 - 2017-04-06 03:52 PM - ralessi

g4jc wrote:

> ralessi wrote:
>
> > This just came to me: Since networkmanager now manages the hostname via systemd-hostnamed, do you think that replacing systemd by openrc would solve this issue?
>
> I'm not sure, since I do not use OpenRC, but it may be worth testing.

I do not either, and didn't dare to try OpenRC on an HD that is entirely encrypted...

> Meanwhile upstream is aware of the issue and it's affect on Tails: https://bugzilla.gnome.org/show_bug.cgi?id=768076

That's great, but would it be enough to disable the transient hostname by setting hostname=none? If I understand well systemd's hostnamectl (https://www.freedesktop.org/software/systemd/man/hostnamectl.html), if a valid static hostname has been set, the transient hostame is not used by hostnamectl.

#15 - 2019-02-28 03:51 PM - bill-auger

- Assignee changed from g4jc to Megver83

- Status changed from open to info needed

while clearing house on the bug tracker, i noticed this BR which is a few years old now - is this still a concern?

i will assign it to megver to ask if indeed he thinks "replacing systemd by openrc would solve this issue", at least for nonprism

#16 - 2019-03-02 07:40 AM - ralessi

I gave up systemd more than two years ago in favor of openrc, and I can say that this solved this issue.