

Packages - Privacy Issue #2037

[networkmanager] Connects to apollo.archlinux.org without asking to check for Connection.

2018-10-12 09:21 AM - vahidrezaborhani

Status:	in progress	% Done:	0%
Priority:	privacy issue		
Assignee:			
Category:			
Description			
hi! (sorry for my english) /usr/bin/NetworkManager frequency connected to apollo.archlinux.org by default and without sending warning or connection request to user. (risk of leaking user IP) networkmanager use it for checking interent connection, so please disabled it by default for user prvicy. tnx.			
Related issues:			
Related to Packages - Privacy Issue #3429: [connman] Contacts a website witho...			confirmed

History

#1 - 2018-10-12 12:18 PM - freemor

- Subject changed from [networkmanager] Please put your reasons here (register first if you haven't) to [networkmanager] Connects to apollo.archlinux.org without asking to check for Connection.

#2 - 2019-02-27 10:37 PM - bill-auger

- Priority changed from bug to privacy issue
- Status changed from open to confirmed

i came across this while refactoring parabolaiso - that heartbeat URL is defined in /etc/NetworkManager/conf.d/20-connectivity.conf - i have added an analogous target file to the parabola repo web root, and set that as heartbeat URL for the LiveISOs

<https://git.parabola.nu/parabolaiso.git/tree/configs/profile/root-image/etc/NetworkManager/conf.d/20-connectivity.conf?h=unified>
https://repo.parabola.nu/check_network_status.txt

AFAIK that is a necessary part of the functionality - its not clear if networkmanager would function properly without that phone-home feature

#3 - 2019-02-28 12:24 AM - eschwartz

NetworkManager works fine without the "connectivity" check enabled, it will simply... not be able to perform connectivity checks to determine whether you are caught behind some silly wifi network's Captive Portal.

See:
https://jlk.fjfi.cvut.cz/arch/manpages/man/NetworkManager.conf.5#CONNECTIVITY_SECTION
https://wiki.archlinux.org/index.php/NetworkManager#Checking_connectivity

And note that it is possible to install a conf.d/ override which disables it, see NetworkManager.conf(5) for more details.

...

By default, the archlinux package for networkmanager is configured to perform this check, and to do so through a server controlled by archlinux.org

Note that this is **NOT** a privacy issue. In the past, access to this file was logged by archlinux.org, this was an accident as we don't intend to retain logs for something we have autoconfigured without asking users whether they wish to connect, and when we realized it was being logged by the nginx defaults, we explicitly disabled the access log via <https://git.archlinux.org/infrastructure.git/commit/?id=68fbaca2ef9f31f624f117899848f4288d6b39d1>

You are of course free to decide that you don't want to rely on our commitment to completely disable logging.

#4 - 2019-02-28 06:43 PM - bill-auger

much like my recent reply to the request for an onion address for the website, this request ignores the fact that pacman necessarily "phones home" every time you use it - it would not work if it did not contact the distro's servers, and you could never upgrade the system - any one who is paranoid about pinging a server that is operated by their distro, probably has not a full grasp of the "big picture" - if you do not trust your distro, then you already have a much larger problem then a simple ping to their webserver

i added the target file to the parabola server as not to ping the arch server - that was probably the appropriate thing to do anyways for any fork; and it

should allow for any parabola system to be fully functional without ever communicating with any 3rd party servers - if it were necessarily communicating with any other 3rd party, i could accept that as a privacy bug

also, as the ping URL can be any other web page on the internet, anyone can of course retain this functionality privately, by changing it point to a server that they operate; or as eli says, the feature can be disabled entirely by each user

lastly, networkmanager is not the only way to connect a parabola system to the internet - there are already alternatives provided, even some user-friendly ones, such the wicd GUI tool

#5 - 2023-01-20 10:45 PM - nona

bill-auger wrote:

much like my recent reply to the request for an onion address for the website, this request ignores the fact that pacman necessarily "phones home" every time you use it - it would not work if it did not contact the distro's servers, and you could never upgrade the system - any one who is paranoid about pinging a server that is operated by their distro, probably has not a full grasp of the "big picture" - if you do not trust your distro, then you already have a much larger problem then a simple ping to their webserver

May be they could use a transparent proxy of some sort and still connect to Parabola? may be it's not about trusting your distro?

also, as the ping URL can be any other web page on the internet, anyone can of course retain this functionality privately, by changing it pint to a server that they operate; or as eli says, the feature can be disabled entirely by each user

What I would like to understand is if it would be possible to apply the reverse logic: privacy by default, functionality by choice (like freedom--and Parabola). May be a little sign after the installation to let users know that they need to enable the ping if they want to break their privacy.

lastly, network manager is not the only way to connect a parabola system to the internet - there are already alternatives provided, even some user-friendly ones, such the wicd GUI tool

Still, the issue of specific software breaking privacy needs to be addressed. As history has shown, the alternatives may disappear. The question is whether it's worth the effort: It's not like I'm going to patch NetworkManager (because it would take me years to understand how to do it safely; I have not even been able to fix my frek*n video), thus I rely on the well-intended people from Parabola, FSF & friends (thanks!).

#6 - 2023-01-21 06:06 AM - bill-auger

- Related to Privacy Issue #3429: [connman] Contacts a website without asking for authorization added

#7 - 2023-01-21 06:08 AM - bill-auger

- Status changed from confirmed to in progress

it was decided long ago that privacy concerns should not be the default - that is the purpose of the nonprism repo - by default, the system should be raw, basic, lean and efficient, and perhaps "dangerous" and so on - those privacy concerns can be addressed every bit as effectively, if they are made to be optional - parabola users have that choice - the distro does no need to impose it

following that line of reasoning to its conclusion, all distros offer complete privacy by default - the loss of privacy represented by this ticket, is forfeited voluntarily, simply by using the public internet - not only do people do that willingly, but then they expect (unreasonably) the local software to somehow conceal their use of a utility, which is necessarily public

the FSDG is very terse on this concern - this is the entirety of its prescriptions, WRT anti-features:

No Malware
The distro must contain no DRM, no back doors, and no spyware.

given that wording, i dont think that the FSDG can be interpreted so strongly to prohibit "keep-alive" connections - the software is not collecting nor conveying any useful information about the user - if the ping events are recorded at all (they probably are not), they are nothing more than a time-stamp associated with an IP address - the conventional "keep-alive" ping does not indicate the identity of the user, nor which computer is being used - the only information conveyed, is that *someone* (whoever that really is) is using a computer connected to the internet, and in some cases, that the computer is located very imprecisely (within perhaps 100 miles radius) of some geographical location

IMHO, those are not the usual "unattended connections" such as a "phone home" feature - they are usually a necessary function of the software, for it's normal use-cases (eg: the desktop GUI indicates when the network becomes connected and disconnected) - regardless that the user may not be aware of how the "online" status is determined, the user does desire those "keep-alive" connections; because the software would be very buggy or undesirable otherwise - that desire disqualifies a keep-alive signal as an "anti-feature" - it is simply a common feature of that and similar tools

however, regardless of the FSDG, i would like to maintain a promise, that parabola users are never required to connect to any internet server, other than those operated by parabola, for all normal uses of the system - IMHO, that is not so much for privacy reasons - its more about being self-sufficient, self-contained - if there is any necessary reason to require users to connect to third-parties, that would indicate that the OS is incomplete (ie: whatever necessary thing is on the third-party server, is something missing from the distro)

in this case, the missing part was simply <https://www.parabola.nu/static/nm-check.txt> - it was missing; but now is merely mis-configured for the

extra/networkmanager and community/connman packages

#8 - 2023-01-21 08:44 PM - nona

Very well explained, as always. Surely, someone with more authority in regards to privacy than /yours truly/ would have a more meaningful discussion about

the loss of privacy represented by this ticket, is forfeited voluntarily, simply by using the public internet

. For example, someone who's reasoning motivates an intranet check or

by changing it point to a server that they operate

. Necessarily,

then (they) already have a much larger problem (than) a simple ping to their webserver

like living in a repressive "democracy". Then, it would be better to be using another operating system (not Parabola) or really knowing your OSI model, kernel, cryptography, etc.

Thank you very much for the enlightening discussion.