Packages - Freedom Issue #1035

[your-system-sanity]: Non-Free Software From Third-party Package Managers

2016-06-19 08:03 PM - jxself

Status:	in progress	**% Done:**	0%
Priority:	feature		
Assignee:	freemor		
Category:			

Description

From a conversation on the gnu-linux-libre mailing list:

http://lists.nongnu.org/archive/html/gnu-linux-libre/2016-04/msg00070.html
http://lists.nongnu.org/archive/html/gnu-linux-libre/2016-04/msg00116.html

"A lot of programming languages have own Package Manager
Examples of those packages managers: npm (CSS/JavaScript), Bower
(Web), pip (Python), Ruby Gems (Ruby),
CPAN (Perl), Cargo (Rust), ..."

These things (like CPAN) would qualify as "repositories" under the Free System Distribution Guidelines. And they do not limit themselves to only including free software. Until/unless Stallman's ideas of either convincing them to only include free software or develop a free replacement come along I propose disabling such things in Parabola.

Related issues:

Related to Packages - Freedom Issue #1413: [gnome-software][discover] offers ...	**in progress**	**2017-07-10**
Related to Packages - Freedom Issue #2304: [wesnoth] Default add-ons server a...	**info needed**	
Related to Packages - Freedom Issue #2260: [openttd] recommends OpenSFX, whic...	**info needed**	
Related to libretools - Feature Request #2403: [libremakepkg]: eradicate mkso...	**info needed**	
Related to Packages - Freedom Issue #123: wanted: blacklist for nonfree aur p...	**not-a-bug**	
Related to Packages - Bug #1904: third-party package managers should not inst...	**open**	
Related to Packages - Freedom Issue #2601: [ruby][rubygems][your-system-sanit...	**fixed**	
Related to Packages - Feature Request #2353: [your-system sanity][python2-pip...	**open**	
Related to Packages - Feature Request #2355: [your-system sanity][0ad] not d...	**open**	
Related to Packages - Feature Request #2356: [your-system sanity][supertux2] ...	**open**	
Related to Packages - Feature Request #2357: [your-system sanity][supertuxkar...	**open**	
Related to Packages - Feature Request #2358: [your-system sanity][freeciv] no...	**open**	
Related to Packages - Feature Request #2359: [your-system sanity][teeworlds] ...	**open**	
Related to Packages - Feature Request #2360: [your-system sanity][xonotic-*] ...	**open**	
Related to Packages - Feature Request #2361: [your-system sanity][minetest] D...	**open**	
Related to Packages - Feature Request #2480: [your system sanity] Make it con...	**in progress**	
Related to Packages - Freedom Issue #194: makepkg license check	**not-a-bug**	
Related to Packages - Freedom Issue #2909: Do check fwupd	**unconfirmed**	
Related to Packages - Freedom Issue #2503: [kodi]: contains nonfree RAR and n...	**confirmed**	
Related to Packages - Freedom Issue #3005: [geoipupdate][sn0int]: TPPM for pr...	**unconfirmed**	
Related to Packages - Freedom Issue #3000: [fwupd]: is an auto-updater , may ...	**unconfirmed**	

History

#1 - 2018-02-09 09:22 AM - asie

I think a better interim solution could be to patch these repository managers so that they only accept free software. However, this does not solve any privacy issues which those packages may cause, as those are not usually documented.

This shouldn't be too hard for some of them; npm for example abides by the SPDX License List standard (https://spdx.org/licenses/). Most of them seem to include licensing information in their packages, though some may not have a standardized way of denoting a specific license.

#2 - 2018-03-17 08:30 PM - bill-auger

also PECL for PHP, cabal-install for haskell, and no doubt various others

blacklisting them would be the "interim solution" - it would be a far larger set of tasks to determine how much work it would be to patch them one-by-one and then to craft and apply the patches

i will add that the FSDG actually prohibits any reference to "third-party repositories that are not committed to only including free software; even if they only have free software today" - so even filtering package according to their licenses may not be fully FSDG-compliant - and bear in mind that the license metadata in these repos is both voluntary and un-verified

as i understand, that is the main reason why parabola does not offer any tools that access the AUR repos - these language-specific repos are much of that same un-supervised, unrestrained, free-for-all sort of dumping ground for literally **whatever**

#3 - 2018-03-17 09:06 PM - bill-auger

i did a shallow survey of the guidelines for several such repos - just to determine the language they use (or neglect) to encourage proper licensing

PERL:
the PERL CPAN and repo guidelines has strong language such as "required" regarding license notices but seems to allow any license

PHP:
PHP PECL had a similarly strong requirement but with notable prescriptions regarding particular licenses; highly suggesting the 'PHP' license and even vaguely prohibiting "wrappers for GPL libraries" while allowing "Wrappers for libraries with license fees or closed sources libraries"

```
Note: wrappers for GPL (all versions) or LGPLv3 libraries will not be accepted.
Wrappers for libraries licensed under LGPLv2 are however allowed while being discouraged.
```

python and ruby:
the language of python PIP and ruby rubygems repo guidelines is significantly weaker saying only that "every package should include a license file"(PIP) and "you should specify a license"(rubygems)

rust:
although the rust cargo metadata file has a key for denoting the license; i could find no place on the web that actually recommends that anyone uses it

haskell:
the haskell cabal repo guidelines has the most libre standard of those i looked at, saying:

```
The code and other material you upload and distribute via this site
must be under an open source license
```

it then includes links to the OSI and FSF for "information about free and open source software licenses" - so perhaps 'cabal-install' is the only of this class that could be retained without conflict

---

for any the others, which do not have such clear and stringent policies as cabal, it would need to be determined, whether it would be theoretically possible (with or without modifications to the package manager) to discern the license of each package before presenting it to the user - it so, then that could be a relatively simple solution, compared to the task of creating and maintaining filtered repos

TODO:

- flatpack
- appimage
- docker
- nuget
- npm
- guix (free culture concerns?)
- asp
- kodi
- are there more?

#4 - 2018-04-26 12:14 AM - bill-auger

- Subject changed from Non-Free Software From Programming Language Package Managers to Non-Free Software From Third-party Package Managers

just to add - this applies not only to language-specific package managers but as well to all third-party package managers such as flatpack, appimage, docker and whatever they cook up next

#5 - 2018-04-26 12:31 AM - bill-auger

- Related to Freedom Issue #1413: [gnome-software][discover] offers non-free software & shows incorrect licenses added

#6 - 2018-07-18 11:08 PM - bill-auger

let us not forget 'nuget'

#7 - 2018-11-29 10:08 PM - bill-auger

i was just reminded that this "elephant in the room" applies even to guix at the intersection of "free software"/"free culture" (i.e. 'your-freedom' ^ 'your-artistic-freedom')

#8 - 2018-11-30 01:26 PM - freemor

Since we package our own pacman perhaps we could create a list of the third party package managers for it. So that if it sees a request to install those it'll throw warnings about:

```
You are installing a third party package manager!
By installing it you assume all responsibility
for system instability it may cause.
Also as doing so bypasses the Parabola blacklist.
You will have to be responsible for checking the
freedom issues of any package you choose to install
with this package manager in the future
```

or something to that effect.

#9 - 2018-11-30 01:44 PM - freemor

From where I sit using a Third party package manager is analogous to using AUR. We can't plug all these holes without creating a frustratingly restricted system. The end user needs to take some responsibility for what they install from non parabola repo places.

Yes, I do see the issue that the TPPMs (got tired of typing it out over and over) are in the Parabola repo. And could be argued as "leading people to non free...". But blacklisting the TPPMs is too restrictive and trying to patch them and then police all the packages that are improperly licensed, etc. would add a huge maintenance load.

Thus I think, Warm strongly up front about the issues possibly with a prompt requiring the user to type "Yes I understand that this may damage my systems stability and that freedom issues are my responsibility" well maybe not that long, but long enough they they have to think about what they are doing rather then just "Y <enter>" because they want to get on with what they were doing.

#10 - 2018-11-30 06:33 PM - freemor

Just a quick note:

eschwartz suggested alpm-hooks as an easy route to implement such warnings.

(mostly here so it doesn't slip from my mind if I choose to revisit this)

#11 - 2018-12-06 10:26 AM - bill-auger

freemor wrote:

> So that if it sees a request to install those it'll throw warnings about:

instead of a warning how about putting them all in a new non-default repo - with your admonishments on a new wiki page describing how to enable the repo

also, the CLI prompt is probably suppressed by pacman GUI front-ends - we could patch octopi but thats not the only one

freemor wrote:

> From where I sit using a Third party package manager is analogous to using AUR.

so should we put AUR GUIs in the new repo with the same warning? - that would seem to be one step in the opposite direction of this issue - it is surely not an omission that there are no AUR helpers in parabola - i think it is clear that AUR helpers, container fetchers, and other package managers should be treated as equivalent - (with the haskell PM being the notable exception above)

freemor wrote:

> blacklisting the TPPMs is too restrictive and trying to patch them

i think a small number of these specify license in metadata - in theory, someone could write a filter - that would be the ideal "rescue" option - still this is several such non-trivial patches against several unfamiliar projects

#12 - 2018-12-06 01:12 PM - freemor

Excellent point about GUI PMs. Living on the CLI I often forget about the GUIs

Separate Repo is an interesting idea. And yes I'd vote to fire AUR helpers in there too. One could easily argue that having a point and click AUR

package manager is "helping people install non-free..."

I do understand about the metadata in some TPPMs. My worry is that not only would the be the patching/maintaining burden that you mentioned to filter, but also a whole layer of then having to police those collections for projects with improper licensing data in their metadata.

#13 - 2019-02-09 06:40 AM - bill-auger

i was just re-reading the FSDG today and it struck me as being quite clear on this issue:

```
Nor should the distribution refer to third-party repositories that are not committed to only
including free software; even if they only have free software today, that may not be true
tomorrow. Programs in the system should not suggest installing nonfree plugins, documentation,
and so on.
```

so again, from my shallow research so far, it looks that the haskell cabal is the only one that we could consider to be "committed to only including free software"

#14 - 2019-02-09 07:11 AM - bill-auger

and FWIW, i also read the original discussion on the FSDG mailing list that occurred about a month before this issue was open, in which RMS suggested that if the repositories themselves could not be convinced to distribute free software only, then the best solution would be to extract the licensing information from each of these package manager's repo indices, if possible, and import only the free packages into a new separate repo for each package manager - that, he also suggested could be hosted by the FSF, if volunteers could accomplish the work of automated filtering

https://lists.nongnu.org/archive/html/gnu-linux-libre/2016-04/msg00116.html

#15 - 2019-02-27 08:03 PM - bill-auger

- Priority changed from freedom issue to discussion

#16 - 2019-02-27 08:18 PM - bill-auger

- Priority changed from discussion to freedom issue

#17 - 2019-02-27 08:18 PM - bill-auger

- Status changed from open to confirmed

#18 - 2019-04-28 11:08 PM - bill-auger

- Related to Freedom Issue #2304: [wesnoth] Default add-ons server allows non-free add-ons added

#19 - 2019-04-28 11:10 PM - bill-auger

- Related to Freedom Issue #2260: [openttd] recommends OpenSFX, which is known to be under a non-FSDG license added

#20 - 2019-07-21 04:15 PM - bill-auger

- Priority changed from freedom issue to feature

- Subject changed from Non-Free Software From Third-party Package Managers to [your-system-sanity]: Non-Free Software From Third-party Package Managers

freemor has been working on an idea tentatively named 'your-system-sanity' to present a more blatant warning about the software that TPPMs index and assist downloading, and the havoc they (especially pip) can wreak on the system, and to identify and isolate them all from the main repos, possibly into new repo like: [unsupported]

though its perhaps not as ideal of a solution that curated repos shared by other distros would be; it is better than the current situation

#21 - 2019-07-21 04:15 PM - bill-auger

- Assignee set to freemor

- Status changed from confirmed to in progress

#22 - 2019-08-01 02:25 AM - bill-auger

- Related to Feature Request #2403: [libremakepkg]: eradicate mksource() from abslibre added

#23 - 2020-01-14 03:00 PM - bill-auger

- Related to Freedom Issue #123: wanted: blacklist for nonfree aur packages added

#24 - 2020-01-14 03:01 PM - bill-auger

- Related to Bug #1904: third-party package managers should not install into /usr/bin added

#25 - 2020-01-14 03:03 PM - bill-auger

- Related to Freedom Issue #2601: [ruby][rubygems][your-system-sanity] Dependencies added

#26 - 2020-01-14 03:03 PM - bill-auger

- Related to Feature Request #2353: [your-system sanity][python2-pip] not detected added

#27 - 2020-01-14 03:03 PM - bill-auger

- Related to Feature Request #2355: [your-system sanity][0ad] not detected added

#28 - 2020-01-14 03:04 PM - bill-auger

- Related to Feature Request #2356: [your-system sanity][supertux2] not detected added

#29 - 2020-01-14 03:04 PM - bill-auger

- Related to Feature Request #2357: [your-system sanity][supertuxkart] not detected added

#30 - 2020-01-14 03:04 PM - bill-auger

- Related to Feature Request #2358: [your-system sanity][freeciv] not detected added

#31 - 2020-01-14 03:04 PM - bill-auger

- Related to Feature Request #2359: [your-system sanity][teeworlds] Downloads packages from server added

#32 - 2020-01-14 03:04 PM - bill-auger

- Related to Feature Request #2360: [your-system sanity][xonotic-] Downloads packages from server added*

#33 - 2020-01-14 03:04 PM - bill-auger

- Related to Feature Request #2361: [your-system sanity][minetest] Downloads packages from server, third-party package manager added

#34 - 2020-01-14 03:05 PM - bill-auger

- Related to Feature Request #2480: [your system sanity] Make it conflict like your-freedom added

#35 - 2020-04-02 01:32 AM - bill-auger

it just ocurred to me that 'asp' would be in this category

#36 - 2020-07-10 07:03 AM - bill-auger

- Related to Freedom Issue #194: makepkg license check added

#37 - 2020-10-11 09:44 AM - bill-auger

- Related to Freedom Issue #2909: Do check fwupd added

#38 - 2020-12-04 09:44 PM - grizzlyuser

What about patching out only the strings in package managers that refer to the domains hosting problematic repositories? PMs themselves can be free software, the problem is just those references to the repos.

It's quite likely they are already made configurable in some of the PMs, like Maven. For those projects lacking repo configuration, a simple one can be requested or even written (and it's a good thing to submit upstream anyway).

If for some given PM there's a public repo that aligns well with the FSDG, then replace upstream repo with that one. If not, then just leave the repo configuration empty and up to the user. Because in many cases, the repo can be, for example, hosted privately by a company, or even locally by a user.

As mentioned before, alpm-hooks can be used to inform users about the necessary configuration.

#39 - 2020-12-05 12:27 AM - bill-auger

that is essentially the solution proposed by RMS (comment # 14) - to have GNU host curated repos for each of these - the task of hacking the client, if necessary, is not a big obstacle - the work involved in creating, curating, and maintaining the thousands of packages, for each of about a dozen package managers, is quite significant though - it would be a rather large and demanding project; and would require long-term dedicated volunteers

#40 - 2020-12-05 07:12 AM - grizzlyuser

I meant just hacking the clients for the time being. Because repo hosting / maintenance is a tremendous effort, obviously. It would be great to have those, but unless there's enough interest from the community, those won't exist.

The point is to give a message that those repos are problematic. It's up to the user to choose the repo they want to use. Whoever needs to use the upstream repos, can always find them, just outside of libre distro.

#41 - 2020-12-05 08:21 AM - bill-auger

ok, i understand the proposal better now - to de-configure the clients, so that they are not usable OOTB; and require each user to configure them to a particular server - i think that is a very good solution - even if there is only one such public server available, it would satisfy the FSDG, by not endorsing it or actively leading users toward it - the 'your-system-sanity' proposal does not meet the FSDG nearly as well

i had a similar idea recently, regarding the AUR - the idea is to customize one of the AUR helpers supported by octopi, such that it does not ever index the AUR, nor connect to it in any way, unless configured by the user to do so, on a single package whitelist basis - only after the user has whitelisted a particular PKGBUILD, would the client connect to it's git repo, for fetching the recipe, and notifying of upgrades - because all AUR PKGBUILDs are in a git repo, the configuration could be maximally general, merely accepting a git URL; and the FSDG would be satisfied, because no software sources would be recommended, or referenced OOTB - that would have the additional benefit of compatibility with any git server, such as github - as long as there is a PKGBUILD in the root dir of the git repo, it would "just work"

it would be relatively simple to accomplish; and simple to use - we would not even need to document how to configure it - the client itself could simply prompt: "Enter a git URL where some PKGBUILD may be fetched: __" - another advantage to that proposal, would be that we would not need to package any of the PCR - we could maintain the PCR in the form of recipes only; and the PCR directory of abslibre could be the default (or only) source for the client's search index

#42 - 2021-01-18 09:24 PM - bill-auger

- Related to Freedom Issue #2503: [kodi]: contains nonfree RAR and nonfree addons added

#43 - 2021-01-18 09:24 PM - bill-auger

i have added 'kodi' to the list #2503 - i added that BR as the blacklist reference about a year ago; because i could find no discussion of it - unfortunately, the kodi team publishes a different set of add-ons for each version, as an indexed repository; which means that someone needs to sort through them upon each new major version release, and re-construct a replacement repo

up until the 'krypton' release, parabola was maintaining a replacement repo for this program - that contained nearly 1000 add-ons - since jan 2019, those 'krypton' add-ons have been obsolete - the current release 'leia' has around 1800 add-ons to sort through; and no one has sorted through them - so currently, no add-ons are available in the parabola 'kodi' - i tried to crudely symlink the existing repo as 'leia'; but it is apparently not working - users will get "Could not connect to repository"

#44 - 2021-01-28 03:32 PM - GNUtoo

I think we could also clarify what users can expect from Parabola at the same time.

I've started to do that here:
https://wiki.parabola.nu/Talk:Main_Page#How_does_Parabola_protects_users_against_nonfree_software

The idea is to make sure users do understand the boundaries of what's handled by Parabola and what's not and point them to other issues that can affect them at the same time to make sure they know about nonfree BIOS and so on (else some users might think that running Parabola is enough to have only free software).

We could also do the same for privacy and security.

Denis.

#45 - 2021-03-23 03:22 PM - telur

some list of TPPM for consideration:

```
pacman -Ss "package manager"
libre/pacman 5.2.2-1.parabola1 (base-devel) [instalita]    A library-based package manager with dependency sup
port
```

```
extra/nuget 5.8.0-1    Package manager for .NET.
community/apm 2.6.1-2    Atom package manager
community/apper 1.0.0-4    An application and package manager using PackageKit
community/bower 1.8.12-1    A package manager for the web
community/dpkg 1.20.5-2    The Debian Package Manager tools
community/dub 1.24.1-1 (dlang)    Developer package manager for D programming language
community/fusesoc 1.12.0-1    Package manager and build abstraction tool for FPGA/ASIC development
community/helm 3.5.3-1    The Kubernetes Package Manager
community/nimble 1:0.12.0-1    Package manager for the Nim programming language
community/npm 7.6.3-1    A package manager for javascript
community/ocaml-findlib 1.8.1-8    OCaml package manager
community/opam 2.0.8-1    OCaml package manager
community/rpm-tools 4.16.1.2-1    RPM Package Manager - RPM.org fork, used in major RPM distros
community/shards 0.13.0-1    The package manager for the Crystal language
community/sn0int 0.20.1-1    Semi-automatic OSINT framework and package manager
pcr/guix 1.1.0-2    A purely functional package manager for the GNU system
pcr/nodejs-bower 1.8.2-1    A package manager for the web
pcr/pacman4console 1.3-1    A 9 level ncurses pacman game with editor, patched not to disturb our package mana
ger and to have
    nice ghosts
```

also maybe putting some pointer in the end of system sanity TPPM block message would be nice like "for further info and feedback see https://labs.parabola.nu/issues/1035"

#46 - 2021-04-03 06:49 AM - bill-auger

- Related to Freedom Issue #3005: [geoipupdate][sn0int]: TPPM for proprietary(?) data added

#47 - 2021-04-03 06:52 AM - bill-auger

re: 'geoipupdate' and 'sn0int' - they may not install anything non-free, and probalby can not corrupt the system; but should probably be investigated

#48 - 2021-04-03 09:16 AM - bill-auger

- Related to Freedom Issue #3000: [fwupd]: is an auto-updater , may also download proprietary firmware added