libretools - Feature Request #3565

[libremakepkg] should have a flag to enable networking during check()

2024-01-08 05:18 PM - lukeshu

Status:	open	**% Done:**	0%
Priority:	feature		
Assignee:			
Category:			

Description

For instance, pcr/python-py3dns doesn't have a check() because py3dns's tests require networking. That's dumb on the authors' parts--it means their test suite is fragile. But nonetheless, it would be good if libremakepkg could run those tests.

It should isolate the filesystem when doing this; if any FS changes are made in check(), they should be hidden from package(); for hermetic-build reasons.

History

#1 - 2024-01-08 05:43 PM - bill-auger

i have considered this, because many programs will fail check() without active networking; but without further hacking, it would open the same security hole which is the reason that networking is disabled during the other stages - namely, because check() runs before package(), it could taint the build - i would put an asterisk beside "should" in the ticket title; because it assumes that tests are always benign - tests normally do expect to have write access to the build tree; so i would propose hacking makepkg to somehow prevent check() from writing to src/ or pkg/ - eg one or a combination of:

- copy the entire build to a new sibling directory of the src/ (eg: check/), exclusively for running check()
- run check() after package(), then delete the packages if check() fails
- run check() as a user other than 'builduser' (eg: 'checkuser')

maybe you can think of others ways to apply paranoia - im not usually a huge fan of paranoia; but this is one place it is appropriate - FWIW, i took the liberty "unilaterally" to modify the main project description on the website to add that promise, and AFAICT, have successfully removed the need for `libremakepkg -N` from all PKGBUILDs - as you probably noticed, in a few cases, that was accomplished by disabling the tests

> All Parabola packages are built from source, in clean chroots, and with networking disabled,

o/c that does not account for arch packages; but i think that is the ideal we should aim for

#2 - 2024-01-08 05:45 PM - lukeshu

Cheaper than creating a full copy would be to use a tmpfs-backed overlayfs. I think systemd-nspawn already has a flag to do that.

#3 - 2024-01-08 06:18 PM - bill-auger

lukeshu wrote:

> I think systemd-nspawn already has a flag to do that.

except that the nonsystemd build of libretools does not use systemd-nspawn - i found that megver's changes for nonsystemd work as well on systemd hosts; so recently i have merged that into the libre build - i planned that the next libretools would not use systemd-nspawn at all

https://git.parabola.nu/packages/libretools.git/commit/?h=wip-2023-12&id=7de6029abaf3673d4130a8fc0adcefb5b17e9706