

Packages - Bug #1527

[archlinux32-keyring] invalid signature

2017-11-14 06:04 PM - bill-auger

| | |
|--|-------------------|
| Status: duplicate | % Done: 0% |
| Priority: bug | |
| Assignee: | |
| Category: | |
| Description when doing a chroot install of an i686 system there are numerous packages rejected with either "unknown trust" or "invalid signature" for Erich Eckner - after populating the pacman keyring like: pacman-key --populate archlinux32 all of the "unknown trust" errors go away but the "invalid signature" remain - but curiously though, if you continue to install the base package repeatedly there will be fewer and fewer rejected packages each time and eventually the install will continue - the first time i tried this building a new ISO it took 6 attempts and the build finally succeeded - after booting the new ISO and it took about 12 attempts then the install succeeded | |
| Related issues: Related to Packages - Bug #2931: [parabola-hackers]: keys are "unknown trust"... fixed Related to Packages - Feature Request #3347: [archlinux-keyring][archlinux32-... open | |

History

#1 - 2017-11-14 07:49 PM - bill-auger

the latest ISO with the archlinux32-keyring pre-installed is here if anyone can help troubleshoot these errors

<https://repomirror.parabola.nu/iso-beta/parabola-systemd-cli-i686-netinstall-2017.11.14-09.33-alpha.iso>

<https://repomirror.parabola.nu/iso-beta/parabola-systemd-cli-i686-netinstall-2017.11.14-09.33-alpha.iso.SHA256SUM>

#2 - 2017-11-14 10:26 PM - bill-auger

a second clean install attempt after well over 40 attempts without succeeding

a third clean install attempt succeeded after about 20 attempts

when trying to upgrade an existing i686 install i had on hardware i had the same errors (full output is in the 'archlinux32-keyring-errors' file attached to the OP)

```
# pacman -Syuu
...
(53/53) checking keys in keyring [#####] 100%
downloading required keys...
:: Import PGP key 4096R/7C98C4C3DE926168DC46FBAA3D06644243BF68D3, "Erich Eckner (just to sign arch packages) <
arch@eckner.net>", created: 2016-04-13? [Y/n]
(53/53) checking package integrity [#####] 100%
error: ncurses: signature from "Erich Eckner (just to sign arch packages) <arch@eckner.net>" is invalid
:: File /var/cache/pacman/pkg/ncurses-6.0+20170902-3-i686.pkg.tar.xz is corrupted (invalid or corrupted packag
e (PGP signature)).
Do you want to delete it? [Y/n]
... (41 more)
```

after installing the 'archlinux32-keyring' package alone and the retrying the upgrade the behavior was the same as the ISO behavior above - repeated runs of 'pacman -Su' would result in fewer and fewer errors each time until eventually the upgrade succeeded - i did not count this time - it was some number of:

```
$ while ! sudo pacman -Su --noconfirm ; do sleep ; done ;
```

#3 - 2017-11-14 11:32 PM - bill-auger

- File archlinux32-keyring-errors added

#4 - 2017-11-15 04:51 AM - oaken-source

I think this might be a mirror issue.

if you use repomirror.parabola.nu, it will redirect you to an arch mirror, whenever possible, which is not what we want for archlinux32 packages. If you use any other mirror, then it works out of the box (at least it did for me)

maybe we should take a look at how repomirror redirects requests, and start redirecting i686 packages to an archlinux32 mirror instead.

#5 - 2017-11-15 05:53 AM - bill-auger

ye p i do think the next step is to find out how the redirector operates - does anyone know where is the code for it? only in place on the server maybe?

#6 - 2017-11-15 05:16 PM - isacdaavid

repomirror.parabola.nu redirects to Parabola mirrors AFAICT, whereas redirector.parabola.nu might take you to Arch ones. both failed on me anyway, even after pacman-key --populate archlinux32-keyring. i can attest that (some) other mirrors don't give this problem.

i think we are hitting the nail here. Bill suggested that the problem might arise as a consequence of signature-package mismatches. it's clear why this would be the case with redirector.parabola.nu, if pacman is trying to match an Arch package (as served by redirector) with an Arch32 signature (as found on our server). outdated Parabola mirrors could be playing a similar role polluting repomirror.parabola.nu's output.

#7 - 2017-11-15 05:25 PM - fauno

not sure how repomirror works, but redirector is just an nginx map that, except for repo databases and [libre] and [pcr] packages, just returns a redirection to another arch mirror. it "randomizes" them by the request time, so there's 10 possible arch mirrors you can get redirected too. repo databases are not redirected otherwise you'll get the original, unfree, arch databases.

so yeah, if arch dropped or is dropping i686 from their repos, this redirections would either give you all 404 or just packages signed by other arch-devs. they shouldn't be invalid signatures though, if you have both archlinux32-keyring and archlinux-keyring installed.

#8 - 2017-11-15 05:27 PM - lukeshu

repomirror: <https://git.parabola.nu/server/repoindex.git/tree/mirror.php>

repomirror.parabola.nu won't send you to an Arch mirror, but redirector.parabola.nu will. redirector.parabola.nu is implemented entirely as an nginx config file:

```
# -*- Mode: nginx; nginx-indent-level: 8; indent-tabs-mode: t -*-

# This is a test version of a simpler redirector
# http://kiwwwi.com.ar/pastes/parabola.lainventoria.com.ar.conf.html

# Map of number with upstream
# Returns a different mirror for every second
map $msec $archlinuxmirror {
    default https://mirrors.uni-plovdiv.net;
    "~1$" https://mirrors.uni-plovdiv.net;
    "~2$" https://foss.aueb.gr/mirrors/linux/archlinux;
    "~3$" https://mirror.f4st.host/archlinux;
    "~4$" https://ftp.fau.de/archlinux;
    "~5$" https://mirror.fluxent.de/archlinux;
    "~6$" https://mirror.fluxent.de/archlinux;
    "~7$" https://arch.jensgutmuth.de;
    "~8$" https://mirror.js-webcoding.de/pub/archlinux;
    "~9$" https://k42.ch/mirror/archlinux;
}

map $msec $parabolamirror {
    default https://repomirror.parabola.nu;
}

server {
    server_name redirector.parabola.nu;
    listen 443 ssl http2;
    listen [::]:443 ssl http2;

    error_log /var/log/nginx/nginx.http.redirector_parabola_nu.error.log error;
    access_log /var/log/nginx/nginx.http.redirector_parabola_nu.access.log specific;

    root /var/empty;

    # Arch Linux 'packages'
    location /core { try_files /bogus @archlinux; }
    location /extra { try_files /bogus @archlinux; }
    location /testing { try_files /bogus @archlinux; }
    location /staging { try_files /bogus @archlinux; }
```

```

location /kde-unstable      { try_files /bogus @archlinux; }
location /gnome-unstable   { try_files /bogus @archlinux; }
location /pool/packages    { try_files /bogus @archlinux; }
location /sources/packages { try_files /bogus @archlinux; }
# Arch Linux 'community'
location /community       { try_files /bogus @archlinux; }
location /community-testing { try_files /bogus @archlinux; }
location /community-staging { try_files /bogus @archlinux; }
location /multilib        { try_files /bogus @archlinux; }
location /multilib-testing { try_files /bogus @archlinux; }
location /multilib-staging { try_files /bogus @archlinux; }
location /pool/community   { try_files /bogus @archlinux; }
location /sources/community { try_files /bogus @archlinux; }
# Parabola (default)
location /                 { try_files /bogus @parabola; }

```

```

# Force database files to be served from Parabola
location ~* \.(db|files|abs)(\.tar\.[gx]z)?$ {
    try_files /bogus @parabola;
}
# Force ARM and MIPS to be served from Parabola
location ~* /(armv7h|mips64el)/ {
    try_files /bogus @parabola;
}

```

```

location @archlinux {
    return 302 $archlinuxmirror$request_uri;
}

```

```

location @parabola {
    return 302 $parabolamirror$request_uri;
}

```

#9 - 2017-11-15 05:29 PM - lukeshu

Is the problem possibly only with arch=('any') packages like we had with ALARM?

#10 - 2017-11-15 05:38 PM - isacdaavid

fauno wrote:

they shouldn't be invalid signatures though, if you have both archlinux32-keyring and archlinux-keyring installed.

can we assume that .sig files are obtained from the same mirror their respective packages are served from?

if this is false then the .sig would come from a trusted Arch key, but the checksum would fail because Arch32 builds aren't bit-identical to Arch's.

#11 - 2017-11-15 05:43 PM - isacdaavid

lukeshu wrote:

Is the problem possibly only with arch=('any') packages like we had with ALARM?

no, see the attached sample output.

#12 - 2017-11-15 06:26 PM - bill-auger

isacdaavid wrote:

can we assume that .sig files are obtained from the same mirror their respective packages are served from?

i looked into that yesterday - i appears that pacman does use the same URL for both package and signature⁰ and aside from a custom front-end callback mechanism that pacstrap probably does not use, the default behavior is to gets the "final_url" var from the redirect URL from curl (CURLINFO_EFFECTIVE_URL)

im not sure if this is related but this happens co-incidentally the same function that throws the many "expected download size exceeded" errors ive been seeing

this is surely related to some conflict across mirrors because as oaken-source noted i can get consistently correct behavior by restricting to a single mirror and consistent failures using the redirector

so for now i am re-building the 32-bit ISOs to use only the isacdaavid.info mirror - that one is very fast (consistently 4-10x faster than any via redirector) and is consistently delivering valid packages - o/c not ideal to hard-code a single mirror but it is the best solution i have found for now

[0]: <https://github.com/anthraxx/pacman/blob/master/lib/libalpm/dload.c#L671>

#13 - 2017-11-15 08:11 PM - isacdaavid

bill-auger wrote:

so for now i am re-building the 32-bit ISOs to use only the isacdaavid.info mirror - that one is very fast (consistently 4-10x faster than any via redirector) and is consistently delivering valid packages - o/c not ideal to hard-code a single mirror but it is the best solution i have found for now

my mirror may go down for a couple minutes every now and then. i don't mind if it goes first, but it would be even better if you followed it with other working mirrors. best of both worlds.

#14 - 2017-11-15 08:20 PM - bill-auger

yea thiits is a slow and tedious process of elimination - that is the one mirror i know now that works - i still have a few more to build so if anyone has found another let me know

hopefully this is just a temporary fix - if the redirector was no longer causing the problem the ISOs that were built previously would probably start working again - so i may not even need to rebuild this new batch can just be deleted

the important thing is that if the redirector is the source of the problem then this is not specific to the ISOs - most existing users are also affected because the redirector is at the top of the default mirrorlist on every system

#15 - 2018-02-13 06:45 PM - bill-auger

for i686 systems:

```
pacman -Sy archlinux32-keyring-transition
```

for a system other than i686:

```
# pacman -U http://pool.mirror.archlinux32.org/i686/core/archlinux32-keyring-transition-20190108-1-any.pkg.tar.xz
```

#16 - 2021-05-14 01:54 PM - bill-auger

- Related to Bug #2931: [parabola-hackers]: keys are "unknown trust" after expiry/renewal added

#17 - 2022-09-24 11:54 AM - bill-auger

- Status changed from open to duplicate

closing in favor of [#1527](#)

#18 - 2022-09-24 11:55 AM - bill-auger

- Related to Feature Request #3347: [archlinux-keyring][archlinux32-keyring][archlinuxarm-keyring]: various problem for parabola added

Files

| | | | |
|----------------------------|---------|------------|------------|
| archlinux32-keyring-errors | 23.4 KB | 2017-11-14 | bill-auger |
|----------------------------|---------|------------|------------|