

Packages - Bug #1344

PGP marginal trust in your-freedom, your-privacy and parabola-keyring

2017-05-26 07:08 PM - bananapie

Status: open	% Done: 0%
Priority: bug	
Assignee:	
Category:	
Description	
<p>I've been getting this message for almost three weeks now. I tried refreshing pacman keys but it didn't work. Folks at IRC told me to report it. :: Starting full system upgrade... resolving dependencies... looking for conflicting packages...</p> <p>Packages (3) parabola-keyring-20170512.1-1 your-freedom-20170525.1-1 your-privacy-20170521-1</p> <p>Total Download Size: 0.12 MiB Total Installed Size: 0.23 MiB Net Upgrade Size: -0.01 MiB</p> <pre>:: Proceed with installation? [Y/n] y :: Retrieving packages... parabola-keyring-20... 107.2 KiB 147K/s 00:01 [-----] 100% your-freedom-201705... 15.4 KiB 308K/s 00:00 [-----] 100% your-privacy-201705... 4.6 KiB 1150K/s 00:00 [-----] 100% (3/3) checking keys in keyring [-----] 100% (3/3) checking package integrity [-----] 100% error: parabola-keyring: signature from "Parabola automatic package builder <dev@lists.parabolagnulinux.org>" is marginal trust :: File /var/cache/pacman/pkg/parabola-keyring-20170512.1-1-any.pkg.tar.xz is corrupted (invalid or corrupted package (PGP signature)). Do you want to delete it? [Y/n] y error: your-freedom: signature from "Parabola automatic package builder <dev@lists.parabolagnulinux.org>" is marginal trust :: File /var/cache/pacman/pkg/your-freedom-20170525.1-1-any.pkg.tar.xz is corrupted (invalid or corrupted package (PGP signature)). Do you want to delete it? [Y/n] y error: your-privacy: signature from "Parabola automatic package builder <dev@lists.parabolagnulinux.org>" is marginal trust :: File /var/cache/pacman/pkg/your-privacy-20170521-1-any.pkg.tar.xz is corrupted (invalid or corrupted package (PGP signature)). Do you want to delete it? [Y/n] y error: failed to commit transaction (invalid or corrupted package (PGP signature)) Errors occurred, no packages were upgraded.</pre>	

History

#1 - 2017-05-30 04:50 PM - clean

I've got the same issue. So I'm no GPG/pacman-key expert, but from best I can tell the dev@lists.parabolagnulinux.org marginal trust key is signed directly by the **ultimate** trusted local key `pacman@localhost`, which means the marginal key is fully valid I think. From what I understand when you sign a key, even if a key is directly signed by your local ultimate trust key, you can still treat it as a marginal trust rather than full. I certainly have not been messing around with pacman-key as root so I don't know how this happened. I could be completely wrong anyway, I'm still a gpg noob.

So far the only way I've heard to fix it is manually changing the trust of dev@lists.parabolagnulinux.org key back to full. I would rather know how the trust got screwed up before doing this though.

EDIT:

So dev@lists.parabolagnulinux.org is signed by pacman's local key with trust level of 4 using `/usr/share/pacman/keyrings/parabola-trusted` as trustdb (done by `pacman-key --populate`) which according to <https://www.gnupg.org/gph/en/manual/x334.html> means it is signed as fully trusted. Thanks to freemor for helping me with that. So I have no idea why it is showing up with only marginal trust. I'll paste the output of `pacman-key --list-sigs dev@lists.parabolagnulinux.org` below, I assume this is safe since it only lists the key id of my local key?

```
gpg: Note: trustdb not writable
pub rsa2048 2014-06-22 [SC]
D3EAD7F9D076EB9AF650149DA170D6A0B669E21A
```

uid [marginal] Parabola automatic package builder <dev@lists.parabolagnulinux.org>
sig 3 A170D6A0B669E21A 2014-06-22 Parabola automatic package builder <dev@lists.parabolagnulinux.org>
sig 456032D717A4CD9C 2014-06-24 Nicolás Reynolds <fauno@endefensadelsl.org>
sig 45698744D4FFBFC9 2014-06-24 Luke T. Shumaker <lukeshu@sbcglobal.net>
sig 7D19D1AFDD312BBE 2014-06-24 keybase.io/encycl <encycl@keybase.io>
sub rsa2048 2014-06-22 []
sig L 739A18D8A9BB7886 2016-10-21 Pacman Keyring Master Key <pacman@localhost>
sub rsa2048 2014-06-22 [E]
sig A170D6A0B669E21A 2014-06-22 Parabola automatic package builder <dev@lists.parabolagnulinux.org>

#2 - 2017-09-09 07:20 PM - lukeshu

From an email I wrote:

I began looking in to why the pacman keyring sometimes thinks that my key is invalid. The key isn't expired, and the parabola-keyring package should have the local Pacman Master Key local-sign it; so it doesn't really make sense. Assuming that everyone who sees this is seeing the *same* bug, the issue seems to be that the validity of the key becomes "Unknown"; that is the keyring says "I trust 'Luke T. Shumaker <lukeshu@sbcglobal.net>', but I'm questioning whether key 99195DD3BB6FE10A2F36ED8445698744D4FFBFC9 really belongs to him." I have no idea how that happens. It doesn't seem to be an issue with the *current* keyring; if you:

```
# rm -rf /etc/pacman.d/gnupg  
# pacman-key --init && pacman-key  
# pacman-key --populate archlinux  
# pacman-key --populate parabola
```

then everything is fine. So, it seems that some version of parabola-keyring that we shipped *in the past* corrupted the keyring in a way that eventually causes this to happen.

I also learned that the gpg manual is woefully incomplete and that the source code is hard to read.

#3 - 2017-09-11 09:29 PM - Raphi111

lukeshu wrote:

```
pacman-key --init && pacman-key
```

Isn't something missing on that line ? What's supposed to be after "&& pacman-key" ? Is it "--refresh" ?

Thanks,

Raphi111

#4 - 2017-09-11 09:36 PM - lukeshu

Oh, yes, my bad. I had meant to write

```
# rm -rf /etc/pacman.d/gnupg  
# pacman-key --init  
# pacman-key --populate archlinux  
# pacman-key --populate parabola
```

I originally was going to do it as a one-liner with &&, but decided to put it on multiple lines, and munged editing it.