Koumbit APT keyring - Bug #15025

main key expired

2014-07-28 14:41 - Antoine Beaupré

Statut:	Rejected	**Début:**	2014-07-28
Priorité:	High	**Echéance:**	
Assigné à:		**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:			
RT ticket:		**Points:**	1
Affected versions:			

Description

the key expired and needs to be renewed.

Demandes liées:

Lié à Koumbit APT keyring - Task #15026: remove old apt key definitively on 2...	**In progress**	**2014-07-28**	**2015-07-28**

Historique

#1 - 2014-07-28 14:44 - Antoine Beaupré

- Statut changé de New à In progress

j'ai généré une clé plus robuste et augmenté l'expiration d'un an, ça donne 1 an au monde pour switcher à l'utilisation de ce package.

```
root@jenkins0:/home/anarcat# sudo -u reprepro -s
reprepro@jenkins0:/home/anarcat$ cd
reprepro@jenkins0:~$ gpg --list-keys
/srv/reprepro/.gnupg/pubring.gpg
--------------------------------
pub   1024D/B7C0A70A 2008-07-11 [expirée : 2014-07-13]
uid                  Koumbit Debian archive autosigning <debian@debian.koumbit.net>

pub   4096R/7B75921E 2009-05-29 [expire : 2016-06-01]
uid                  Antoine Beaupré <anarcat@koumbit.org>
uid                  Antoine Beaupré <anarcat@debian.org>
uid                  Antoine Beaupré (work) <anarcat@koumbit.org>
uid                  Antoine Beaupré (home address) <anarcat@anarcat.ath.cx>
uid                  Antoine Beaupré <anarcat@orangeseeds.org>
uid                  Antoine Beaupré (Debian) <anarcat@debian.org>
sub   2048R/AFD0FDF8 2012-07-24
sub   2048R/D2DF2587 2012-07-18
sub   2048R/EE02855A 2012-07-20
sub   4096R/9C5A5581 2009-05-29 [expire : 2016-06-01]

pub   2048R/92A624F7 2013-02-19 [expire : 2017-02-20]
uid                  Jenkins autobuilder <jenkins@jenkins.koumbit.net>
sub   2048R/8B07F371 2013-02-19 [expire : 2017-02-20]

reprepro@jenkins0:~$ gpg --gen-key
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Sélectionnez le type de clef désiré :
   (1) RSA et RSA (par défaut)
   (2) DSA et Elgamal
   (3) DSA (signature seule)
   (4) RSA (signature seule)
Quel est votre choix ? 1
les clefs RSA peuvent faire entre 1024 et 4096 bits de longueur.
Quelle taille de clef désirez-vous ? (2048) 4096
La taille demandée est 4096 bits
Veuillez indiquer le temps pendant lequel cette clef devrait être valable.
         0 = la clef n'expire pas
      <n>  = la clef expire dans n jours
      <n>w = la clef expire dans n semaines
```

```
      <n>m = la clef expire dans n mois
      <n>y = la clef expire dans n ans
Pendant combien de temps la clef est-elle valable ? (0) 3y
La clef expire le jeu 27 jui 2017 14:24:00 EDT
Est-ce correct ? (o/N) o

Une identité est nécessaire à la clef ; le programme la construit à partir
du nom réel, d'un commentaire et d'une adresse électronique de cette façon :
   « Heinrich Heine (le poète) <heinrichh@duesseldorf.de> »

Nom réel : Koumbit Debian archive autosigning
Adresse électronique : debian@debian.koumbit.net
Commentaire :
Vous avez sélectionné cette identité :
    « Koumbit Debian archive autosigning <debian@debian.koumbit.net> »

Faut-il modifier le (N)om, le (C)ommentaire, l'(A)dresse électronique
ou (O)ui/(Q)uitter ? p
Faut-il modifier le (N)om, le (C)ommentaire, l'(A)dresse électronique
ou (O)ui/(Q)uitter ? o
Une phrase de passe est nécessaire pour protéger votre clef secrète.

Vous ne voulez pas de phrase de passe — c'est sans doute une *mauvaise*
idée. C'est possible quand même. Vous pouvez modifier la phrase de passe
à tout moment en utilisant ce programme avec l'option « --edit-key ».

De nombreux octets aléatoires doivent être générés. Vous devriez faire
autre chose (taper au clavier, déplacer la souris, utiliser les disques)
pendant la génération de nombres premiers ; cela donne au générateur de
nombres aléatoires une meilleure chance d'obtenir suffisamment d'entropie.
+++++
..+++++
De nombreux octets aléatoires doivent être générés. Vous devriez faire
autre chose (taper au clavier, déplacer la souris, utiliser les disques)
pendant la génération de nombres premiers ; cela donne au générateur de
nombres aléatoires une meilleure chance d'obtenir suffisamment d'entropie.
..............+++++
......+++++
gpg: clef 29DA8118 marquée de confiance ultime.
les clefs publique et secrète ont été créées et signées.

gpg: vérification de la base de confiance
gpg: 3 marginale(s) nécessaire(s), 1 complète(s) nécessaire(s),
     modèle de confiance PGP
gpg: profondeur : 0  valables :   1  signées :   0
     confiance : 0 i., 0 n.d., 0 j., 0 m., 0 t., 1 u.
gpg: la prochaine vérification de la base de confiance aura lieu le 2017-07-27
pub   4096R/29DA8118 2014-07-28 [expire : 2017-07-27]
 Empreinte de la clef = 6FEA D189 28B5 7203 8F2B  DA08 A59D 9792 29DA 8118
uid                  Koumbit Debian archive autosigning <debian@debian.koumbit.net>
sub   4096R/67D14AC1 2014-07-28 [expire : 2017-07-27]

reprepro@jenkins0:~$ gpg --edit-key 0x6DC388D8B7C0A70A
gpg (GnuPG) 1.4.12; Copyright (C) 2012 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

La clef secrète est disponible.

pub  1024D/B7C0A70A  créé : 2008-07-11  expirée : 2014-07-13  utilisation : SC
                     confiance : inconnu       validité : expirée
sub  2048g/554181B9  créé : 2008-07-11  expirée : 2014-07-13  utilisation : E
[ expirée ] (1). Koumbit Debian archive autosigning <debian@debian.koumbit.net>

gpg> expire
Modification de la date d'expiration de la clef principale.
Veuillez indiquer le temps pendant lequel cette clef devrait être valable.
         0 = la clef n'expire pas
      <n>  = la clef expire dans n jours
      <n>w = la clef expire dans n semaines
      <n>m = la clef expire dans n mois
      <n>y = la clef expire dans n ans
Pendant combien de temps la clef est-elle valable ? (0) 1y
La clef expire le mar 28 jui 2015 14:27:17 EDT
Est-ce correct ? (o/N) o
```

```
pub  1024D/B7C0A70A  créé : 2008-07-11  expire : 2015-07-28  utilisation : SC
                     confiance : inconnu       validité : inconnu
sub  2048g/554181B9  créé : 2008-07-11  expirée : 2014-07-13  utilisation : E
[ inconnue] (1). Koumbit Debian archive autosigning <debian@debian.koumbit.net>

gpg> save
reprepro@jenkins0:~$ gpg --default-key 29DA8118 --sign-key B7C0A70A

gpg: vérification de la base de confiance
gpg: 3 marginale(s) nécessaire(s), 1 complète(s) nécessaire(s),
     modèle de confiance PGP
gpg: profondeur : 0  valables :   1  signées :   0
     confiance : 0 i., 0 n.d., 0 j., 0 m., 0 t., 1 u.
gpg: la prochaine vérification de la base de confiance aura lieu le 2017-07-27
pub  1024D/B7C0A70A  créé : 2008-07-11  expire : 2015-07-28  utilisation : SC
                     confiance : inconnu       validité : inconnu
sub  2048g/554181B9  créé : 2008-07-11  expirée : 2014-07-13  utilisation : E
[ inconnue] (1). Koumbit Debian archive autosigning <debian@debian.koumbit.net>

pub  1024D/B7C0A70A  créé : 2008-07-11  expire : 2015-07-28  utilisation : SC
                     confiance : inconnu       validité : inconnu
Empreinte clef princip. : AD05 6990 EB84 21EB EFC6  EC9E 6DC3 88D8 B7C0 A70A

     Koumbit Debian archive autosigning <debian@debian.koumbit.net>

Cette clef va expirer le 2015-07-28.
Voulez-vous vraiment signer cette clef avec votre
clef « Koumbit Debian archive autosigning <debian@debian.koumbit.net> » (29DA8118)

Voulez-vous vraiment signer ? (o/N) o

reprepro@jenkins0:~$ gpg --default-key B7C0A70A  --sign-key  29DA8118

gpg: vérification de la base de confiance
gpg: 3 marginale(s) nécessaire(s), 1 complète(s) nécessaire(s),
     modèle de confiance PGP
gpg: profondeur : 0  valables :   1  signées :   1
     confiance : 0 i., 0 n.d., 0 j., 0 m., 0 t., 1 u.
gpg: profondeur : 1  valables :   1  signées :   0
     confiance : 1 i., 0 n.d., 0 j., 0 m., 0 t., 0 u.
gpg: la prochaine vérification de la base de confiance aura lieu le 2015-07-28
pub  4096R/29DA8118  créé : 2014-07-28  expire : 2017-07-27  utilisation : SC
                     confiance : ultime        validité : ultime
sub  4096R/67D14AC1  créé : 2014-07-28  expire : 2017-07-27  utilisation : E
[  ultime ] (1). Koumbit Debian archive autosigning <debian@debian.koumbit.net>

pub  4096R/29DA8118  créé : 2014-07-28  expire : 2017-07-27  utilisation : SC
                     confiance : ultime        validité : ultime
Empreinte clef princip. : 6FEA D189 28B5 7203 8F2B  DA08 A59D 9792 29DA 8118

     Koumbit Debian archive autosigning <debian@debian.koumbit.net>

Cette clef va expirer le 2017-07-27.
Voulez-vous vraiment signer cette clef avec votre
clef « Koumbit Debian archive autosigning <debian@debian.koumbit.net> » (B7C0A70A)

Voulez-vous vraiment signer ? (o/N) o

reprepro@jenkins0:~$ gpg --keyserver pool.sks-keyservers.net --send-keys 29DA8118 B7C0A70A
gpg: envoi de la clef 29DA8118 au serveur hkp pool.sks-keyservers.net
gpg: envoi de la clef B7C0A70A au serveur hkp pool.sks-keyservers.net
reprepro@jenkins0:~$ gpg --keyserver ha.pool.sks-keyservers.net --send-keys 29DA8118 B7C0A70A
gpg: envoi de la clef 29DA8118 au serveur hkp ha.pool.sks-keyservers.net
gpg: envoi de la clef B7C0A70A au serveur hkp ha.pool.sks-keyservers.net
```

#2 - 2014-07-28 14:53 - Antoine Beaupré

j'ai signé la clef avec ma clé personnelle en copiant le fingerprint de la nouvelle clé, puis je l'ai remise sur les keyservers et redownloadée sur jenkins.

je travaille a inclure ca dans le package debian.

#3 - 2014-07-28 15:59 - Antoine Beaupré

- Statut changé de In progress à Needs documentation

il reste à documenter comment faire cette procédure à l'avenir... pas simple!

mais bon, c'est fait: le key.asc a les deux clés, ainsi que le package debian.

il faut aussi ouvrir un ticket pour retirer la clé 1024b dans 1 an.

#4 - 2014-07-28 17:12 - Antoine Beaupré

les tickets sont cleanés.

#5 - 2014-07-28 17:20 - Antoine Beaupré

- Statut changé de Needs documentation à Postponed

j'ai mis un indice ici: https://wiki.koumbit.net/JenkinsMaintenance#Renouveler_la_clef_PGP_de_reprepro

... mais peut-être qu'il faudrait une page RepreproMaintenance...

j'ai créé un ticket pour la suite dans Redmine:15026. je remets à plus tard l'exercice de docu pour le reste, je pense qu'on est corrects.

#6 - 2015-08-18 18:26 - Antoine Beaupré

this did **not** work because jenkins is still using the old key.

i put default-key 6FEAD18928B572038F2BDA08A59D979229DA8118 in the gpg.conf, hoping this will fix it.

#7 - 2015-08-18 18:30 - Antoine Beaupré

to regenerate the .gpg files:

```
reprepro export unstable
reprepro export testing
reprepro export stable
```

#8 - 2015-08-18 18:31 - Antoine Beaupré

- Statut changé de Postponed à Needs documentation

- Assigné à Antoine Beaupré supprimé

this needs to be turned into documentation, in:

https://wiki.koumbit.net/RepreproConfiguration#PGP (or *Maintenance?) and
https://wiki.koumbit.net/JenkinsMaintenance#Renouveler_la_clef_PGP_de_reprepro

#9 - 2019-10-02 15:13 - Gabriel Filion

- Statut changé de Needs documentation à Rejected