



[Accueil](#) [Services](#) [Equipe](#) [Références](#) [Partenaires](#) [Contact](#) [OctoBlog](#) [Docs](#)

apt-mirror : BADSIG on security.debian.org (with solution)

Le 26 November 2010 , par Benjamin Sonntag,

At Octopuce, we are Debian professional and are using Debian everywhere we can. For one of our customers, we maintained a mirror of Debian repositories, which are used by internal Linux servers.

This mirror is using apt-mirror since we cannot access the Internet by rsync or ftp protocol : we have to use http to mirror the repositories.

A few days ago, I saw the following error message on a Linux Debian server using this internal mirror :

```
W: GPG error: http://fr-debianmirror lenny/updates Release:
The following signatures were invalid: BADSIG
9AA38DCD55BE302B Debian Archive Automatic Signing Key
(5.0/lenny) <ftpmaster@debian.org>
W: You may want to run apt-get update to correct these
problems
```

This issue was critical : the GPG signature of debian security repository was incorrect !! There were 3 places where this could happen :

- ▶ At the Debian repository security.debian.org : I don't think so, or google would have told me ;)
- ▶ During the mirroring process : maybe ...
- ▶ At the final server location : each Debian machine have a GPG keyring of allowed keys for repository signature. The apt-key tool is used to manage this keyring, located at /etc/apt/trusted.gpg and /etc/apt/trustdb.gpg

check apt-key configuration

First, check if the command "apt-key list" tell you that the faulty key is allowed. If it is not, you may add it by installing the proper debian package, for example :

```
aptitude install debian-archive-keyring
```

some people in the Internet tell you to use `gpg --keyserver keyserver.fr --recv-key 0x9AA38DCD55BE302B | apt-key add -`

but using the debian package should work "the right way" :)

Check the mirror

Of course, our Debian servers were properly installed, so we already had the ftpmaster Debian archive GPG key in our servers.

Next step: I checked the faulty file : it was located at /var/spool/apt-mirror/mirror/security.debian.org/debian-security/dists/lenny/updates/Release.gpg

Sur l'OctoBlog

[Octopuce SARL recherche un développeur PHP/MySQL](#) (le 17 novembre 2011 , par Saïd Bouaïssi, Benjamin Sonntag,
[Octopuce à Metz \(Libre et Entreprises\)](#) (le 23 octobre 2011 , par Chantal Bernard-Putz,
[Comment utiliser les hooks de GIT pour mettre à jour automatiquement un site de développement](#) (le 19 janvier 2011 , par Benjamin Sonntag,

Logiciels Libres ?

Acteurs du Libre les membres de l'équipe Octopuce participent à divers projets, soit au nom de l'entreprise soit en leur nom propre, sur le temps offert à l'équipe pour conduire des projets personnels.

Nous avons contribué, dès ses débuts, à la conception et mise en oeuvre de la plateforme [AlternC, panneau de contrôle web](#) sur une bases 100% libre. Cette plateforme nous la proposons pour votre hébergement mutualisé ou dédié. De la même manière est né [Dmanager](#), logiciel de partage de fichiers via internet.

C'est ainsi que pour vos projets Octopuce privilégie le choix de solutions et logiciels libres quand ceux-ci répondent à vos besoins. L'ensemble des développements réalisés pour vous sous licence libre sont mis à la disposition de tous.

Une référence ?



Axance est une société spécialisée dans l'ergonomie

et l'accessibilité des sites web. Cette agence web fait partie de ceux qui, nous ayant fait confiance de longue date, ont pu profiter de notre expertise technique destinée aux agences.

This file should be a GPG signature of the Release file, located in the same directory.

There, I saw this :

```
.../debian-security/dists/lenny/updates/$ ls -l
-rw-r--r-- 1 apt-mirror 835 2010-10-20 10:13 Release.gpg
-rw-r--r-- 1 apt-mirror 40K 2010-11-22 21:12 Release
```

And here it looks obvious to me we have a problem: a signature cannot be older than the file it is signing !

In fact, our apt-mirror (which is using wget to download files) is using a proxy server to connect to the official Debian mirrors. As such, I put the following in /etc/wgetrc :

```
http_proxy = http://10.42.12.12:8080/
```

and here is the problem: this proxy is unable to detect when the release.gpg file has been modified, and as such, he often returns an old version of this file !

To check this theory, I used wget with -S to see the HTTP headers returned by the server and the proxy :

```
fr-debianmirror:/tmp# wget http://security.debian.org
/debian-security/dists/lenny/updates/Release.gpg -S
--2010-11-26 12:08:43-- http://security.debian.org/debian-
security/dists/lenny/updates/Release.gpg
Connecting to 10.42.12.12:8080... connected.
Proxy request sent, awaiting response...
HTTP/1.1 200 OK
Date: Fri, 26 Nov 2010 10:57:06 GMT
Server: Apache
Last-Modified: Mon, 20 Oct 2010 10:13:36 GMT
ETag: "343-e08fc449a1532"
Accept-Ranges: bytes
Content-Type: text/plain
Content-Length: 835
Connection: close
Age: 855
Length: 835 [text/plain]
```

the lines in bold are the guilty one : the last modified date is not the right one, and the Age header tells us how old in the proxy cache is this entry.

Our solution

So, the solution was to tell wget to ask the proxy for a fresh version by using the `--no-cache` directive. A better way to use this is to add this line to /etc/wgetrc :

```
cache = off
```

and here we are :

```
wget http://security.debian.org/debian-security/dists/lenny
/updates/Release.gpg -S
--2010-11-26 12:17:39-- http://security.debian.org/debian-
security/dists/lenny/updates/Release.gpg
Connecting to 10.42.12.12:8080... connected.
Proxy request sent, awaiting response...
HTTP/1.1 200 OK
Date: Fri, 26 Nov 2010 11:05:58 GMT
```



PricewaterhouseCoopers (« PwC ») développe en France des missions d'audit, d'expertise comptable et de conseil pour des entreprises de toutes tailles, publiques et privées. Octopuce est en charge de l'administration système des serveurs Linux de PwC France.

Server: Apache
Last-Modified: Mon, 22 Nov 2010 20:12:36 GMT
ETag: "343-495a9e08a1500"
Accept-Ranges: bytes
Content-Type: text/plain
Content-Length: 835
Connection: close
Age: 0
Length: 835 [text/plain]

[Haut de page](#) | [Accueil](#) | [Services](#) | [Contact](#)

© Copyright 1999-2012 Octopuce