Packages - Bug #933

Outdated mirrors security issue.

2016-02-14 06:49 PM - GNUtoo

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

Description

Hi,

We had this mirror in /etc/pacman.d/mirrorlist as the first(default) mirror:

```
http://parabolagnulinux.mirrors.linux.ro/$repo/os/$arch
```

The issue is that it stopped being up to date.
/etc/pacman.d/mirrorlist comes from libre/pacman-mirrorlist.
Here we assume that the user kept the default configuration.
When that mirror stopped being up to date, pacman still used it to check for updates, and will still do for as long as that mirror is still online.
It only uses that mirror since it's available online and it's the first/default one.
Computers still using that mirror do not have an up to date system.
They will continue to do so, until the user finds the lack of update suspicous enough to bother checking what happened, unless we:

- Warn the users.
- Fix Parabola to prevent such issue from happening again.

Here the mirror is not necessarily malicious. It could just have had an issue and stop syncing.
Parabola should be resilient to that, either automatically, or with the help of people like its developers or community.

We should prevent systems from not learning about new updates:

- First by addressing that concern assuming that the mirrors are not malicious, that also assume possible MITM.
- Then by addressing the malicious mirrors concerns.

As parabola infrastructure was down when I found that issue, I sent a mail to the [DEV] mailing list, but the mail delivery was delayed due to the infrastructure being down.
Its subject is "[Dev] Mirrors vulnerability issue, Many outdated installs in the wild"

Related issues:

Related to Packages - Bug #1107: My Parabola OS doesn't update packages	**fixed**	**2016-09-22**

History

#1 - 2016-02-14 07:07 PM - GNUtoo

MITM prevention:
To prevent MITM we need to enforce https or onion services for all mirrors in mirrorlist.
I however don't know how to make sure https is secure by default, server side and client side.
https is very configurable, and on some configuration it doesn't prevent a MITM from downgrading the ciffer suite to NULL (clear text) or to a breakable cipher.

Making sure pacman -Sy has the lastest db files:
I've no idea if the .db are signed. But even if they are this doesn't fix that issue, since, actually, the db are downloaded form the mirrors.
So assuming a mirror is too old, the db are still signed with valid signatures.

libre/reflector is a tool to update the mirrorlist. There might be a way to use it to make parabola systems to automatically find the right mirror. Such tool would have to be enabled by default.
As such, it would have to be rock solid.
It would also need to be integrated into the dependencies of the "base" package without any downsides.
Downsides typically include pulling a lot of other dependencies, or since it's a python(3) program, increased RAM usage and performances issues on slower systems(like ARM, with very few RAM and a really slow storage(like microSD).

Another way to do it is trough redirection, on the dev mailing list, there is a thread about using redirection to spread the mirrors load. This however can also be used to make sure that systems have the lastest mirrorlist package.

The thread is named "[Dev] [announcement] mirror redirector available for testing"
This would probably address the malicious mirrors nicely.

Yet another way to do it would be to make parabola infrastructure server the mirrorlist pacakge.
However I wonder what would happen if a malicious mirror starts serving an older mirrorlist.
It could do that by serving a snapshot that is from before the move of the mirrorlist to the parabola infrastructure
It could also do it by with some MITM between the user and the server hosting that mirrorlist, in order to trick pacman into thinking it's a mirror that only hosts (an old) mirrorlist. Pacman might not be able to prevent that.

#2 - 2016-02-15 02:36 PM - GNUtoo

To explain the security issue better, let's take a real example:
We have iceweasel 1:43.0 for all architectures in that mirror:

```
http://parabolagnulinux.mirrors.linux.ro/libre/os/i686/iceweasel-1%3a43.0.deb1-1-i686.pkg.tar.xz
```

On other mirrors we have:

```
libre/iceweasel 1:44.0.deb1-1

pacman -Q -i iceweasel
```

gives me

```
http://packages.debian.org/sid/iceweasel
```

for its website.
Let's consult the ChangeLog:

```
iceweasel (44.0-1) unstable; urgency=medium

  * New upstream release.
  * Fixes for mfsa2016-{01-04,06,09-11}, also known as:
    CVE-2016-1930, CVE-2016-1931, CVE-2016-1933, CVE-2016-1935,
    CVE-2016-1939, CVE-2016-1937, CVE-2016-1942, CVE-2016-1943,
    CVE-2016-1944, CVE-2016-1945, CVE-2016-1946, CVE-2016-1947.

  * js/src/jit/mips-shared/Architecture-mips-shared.h,
    js/src/jit/mips-shared/Assembler-mips-shared.*,
    js/src/jit/mips32/Architecture-mips32.*,
    js/src/jit/mips32/Assembler-mips32.*,
    js/src/jit/mips64/Architecture-mips64.*,
    js/src/jit/mips64/Assembler-mips64.*: Fix build failure on mipsel.
    bz#1213146.

 -- Mike Hommey <glandium@debian.org>  Wed, 27 Jan 2016 11:12:44 +0900

iceweasel (43.0.4-1) unstable; urgency=medium
[...]
```

To get the addresses I enter the CVE in https://cve.mitre.org/cve/cve.html
Several CVE link to the same mozilla security advisory, because theses advisories are for several similar bugs.
If we only list the criticlal ones with potentially arbitrary remote code execution we have:

- https://www.mozilla.org/en-US/security/advisories/mfsa2016-01/
- https://www.mozilla.org/en-US/security/advisories/mfsa2016-03/
- https://www.mozilla.org/en-US/security/advisories/mfsa2016-10/

This needs to be fixed, else users will still keep using the old versions of iceweasel.

I guess many more packages are affected, we can use the same methodology to find out.

#3 - 2016-09-22 09:32 PM - isacdaavid

- Related to Bug #1107: My Parabola OS doesn't update packages added