Arch Linux Security Projects

Remi Gacogne

November 10, 2015

About me

- Remi Gacogne
- Software Engineer @ PowerDNS
- Teaching C / HA @ Epita, Web Security @ Ionis-STM
- Used to be a SysAdmin, I know uptime matters
- Linux user since 2001 (Arch, CentOS, Debian, Fedora, Mandrake, Slackware)
- rgacogne on IRC (OFTC, Freenode)

Do you know what the Arch Linux Security Team does?

Plan

Tracking Vulnerabilities

- One year of ASAs
- The easy way
- The hard way
- Fixing issues

Reproducible builds

- What?
- Why?
- How?

Hardening Arch

- Hardening binaries
- Protecting pacman’s database

Tracking Vulnerabilities

A bit of history

Roughly one year ago:

- Levente and I: “hey, it’s great to have CVE Monitoring, and we would like to build on that to have security advisories, how can we help?”
- Allan: “it’s not going to happen”
- Allan: “if you want to have security advisories in Arch, do it yourself, because no one else is going to, as there is no glory in it”

Aaaand there goes my free time..

Well

VULNERABILITIES
VULNERABILITIES EVERYWHERE
imgflip.com

Advisories

```
Arch Linux Security Advisory ASA-201510-9
=========================================
Severity: Critical
Date    : 2015-10-15
CVE-ID  : CVE-2015-5291
Package : mbedtls
Type    : arbitrary code execution
Remote  : Yes
Link    : https://wiki.archlinux.org/index.php/CVE

Summary
=======
The package mbedtls before version 2.1.2-1 is vulnerable to remote code execution.

Resolution
==========
Upgrade to 2.1.2-1.

# pacman -Syu ``mbedtls>=2.1.2-1''

The problem has been fixed upstream in versions 2.1.2, 1.3.14 and 1.2.17.

Workaround
==========

To be protected against this vulnerability, you need to...

Description
===========

When the client creates its ClientHello message, due to insufficient
bounds checking it can overflow the heap-based buffer containing the
message while writing some extensions...
```

A bit of history

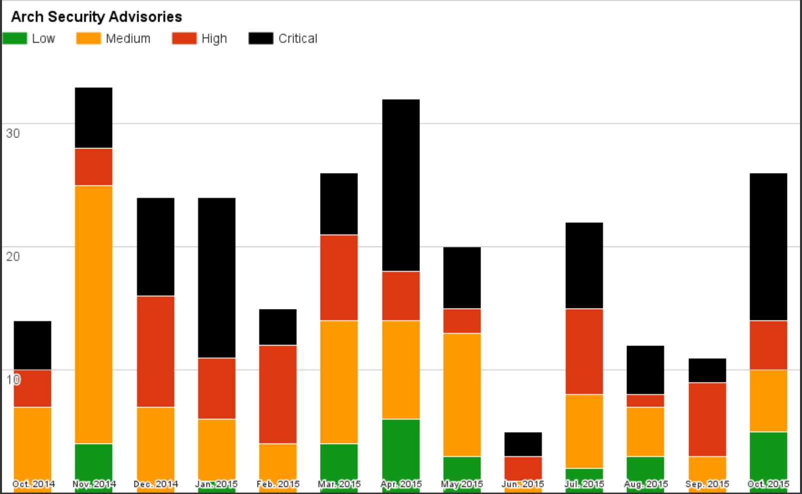
One year later..

- What started as an unofficial project got endorsed by Arch
- No rage-quit (yet)
- Advisories are listed on LWN.net

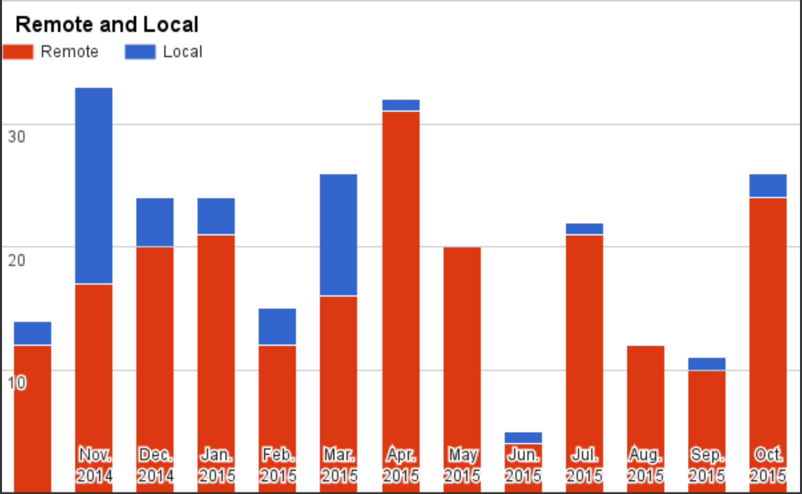
The team:

- Christian Rebischke (shibumi)
- Levente Polyak (anthraxx), also a TU
- Remi Gacogne (rgacogne)
- a lot of people in the shadow (thanks!)

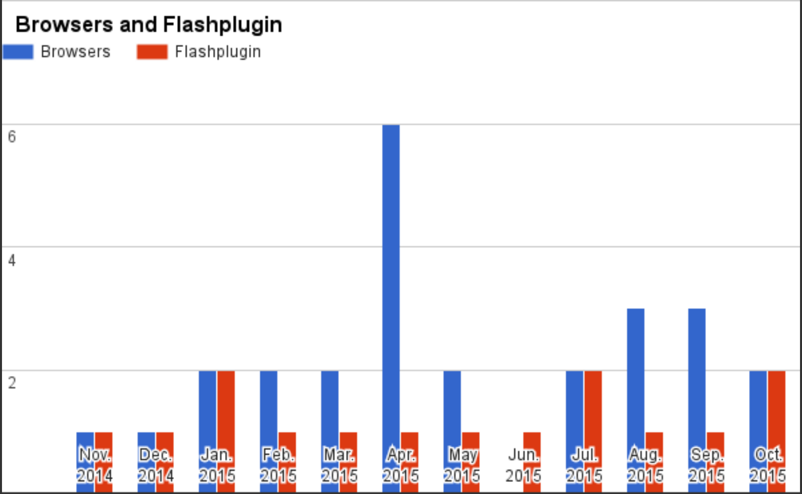
Advisories


Arch Security Advisories
Low
Medium
High
Critical
30
20
10
Oct. 2014
Nov. 2014
Dec. 2014
Jan. 2015
Feb. 2015
Mar. 2015
Apr. 2015
May 2015
Jun. 2015
Jul. 2015
Aug. 2015
Sep. 2015
Oct. 2015

Remote vulnerabilities



Browsers and flash



Tracking vulnerabilities the easy way

We are lazy, so let's try using automated tools:

- Matching packages against vulnerability databases
- Mitre, OSVDB, Red Hat, NVD..
- https://github.com/jelly/ArchCVE

Unfortunately..

Tracking vulnerabilities the hard way

Well, looks like we still need some manual monitoring:

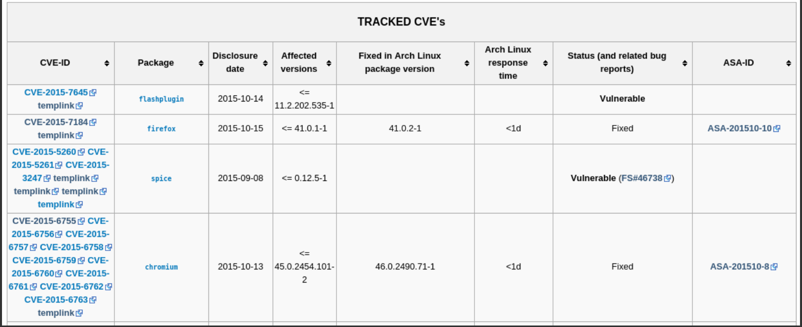
- Reading changelogs
- Following public ML (bugtraq, full-disclosure, oss-sec)
- Following private ML (distros, linux-distros)

Tracking vulnerabilities the hard way

A new vulnerability has been found in a package we ship, what now?

- Update the CVE page
- Fix the issue in Arch

Updating the CVE page



TRACKED CVE's

CVE-ID	Package	Disclosure date	Affected versions	Fixed in Arch Linux package version	Arch Linux response time	Status (and related bug reports)	ASA-ID
CVE-2015-7645 templink	flashplugin	2015-10-14	<= 11.2.202.535-1			**Vulnerable**	
CVE-2015-7184 templink	firefox	2015-10-15	<= 41.0.1-1	41.0.2-1	<1d	Fixed	ASA-201510-10
CVE-2015-5260 CVE-2015-5261 CVE-2015-3247 templink templink templink templink	spice	2015-09-08	<= 0.12.5-1			**Vulnerable** (FS#46738)	
CVE-2015-6755 CVE-2015-6756 CVE-2015-6757 CVE-2015-6758 CVE-2015-6759 CVE-2015-6760 CVE-2015-6761 CVE-2015-6762 CVE-2015-6763 templink	chromium	2015-10-13	<= 45.0.2454.101-2	46.0.2490.71-1	<1d	Fixed	ASA-201510-8

Fixing issues

Okay, how do we fix the security issue?

- Often, it has already been fixed, because Arch updates really fast.

Otherwise:

- Does a fix exist?
- Has a new version been released with that fix?

Fixing issues

If a new version is available:

- Flag the package as out-of-date, mentioning this is a security update
- After some time, open a bug and add the bug number to the CVE page
- Bully the packager via mail / IRC (hint: don't do it)
- For community packages, Levente might fix the issue himself

Fixing issues

If a fix is available, but not included in any release yet:

- Don't flag the package as out-of-date
- Open a bug, with the security issue and a link to the fix, and add the bug number to the CVE page
- Bully the packager via mail / IRC (hint: still a big no-no)

Fixing issues

When there is no fix available:

- Don't flag the package as out-of-date
- Don't open a bug
- Search the relevant ML, take a look at what well-funded distros are doing
- Propose a patch upstream yourself if you know what you are doing

Writing the advisory

The issue has been fixed, the package is out of testing:

- Someone in the Security team takes ownership by scheduling an ASA
- Researchs the technicals details
- Writes and issues the advisory

Reproducible Builds

What are reproducible builds?

"Reproducible builds are a set of software development practices which create a verifiable path from human readable source code to the binary code used by computers."[1]

[1] `http://reproducible-builds.org`

Why do we want reproducible builds?

Arch uses binary packages:

- We don’t have to trust the mirrors, thanks to package signing
- We don’t have to trust the network either, thanks to package signing again
- However, we need to trust the Trusted Users and Developers
- More importantly, we need to trust the hosts they build their packages on (pkgbuild.com, anyone?)

With reproducible builds, we can check that the binary packages matches the intended source code.

How do we get reproducible builds?

Reproduce the build on another host, and check that there is no difference.

- Get the PKGBUILD via abs or the git repository
- Build using makechrootpkg
- Check the cryptographic fingerprints of the files in the resulting package against those of the original one

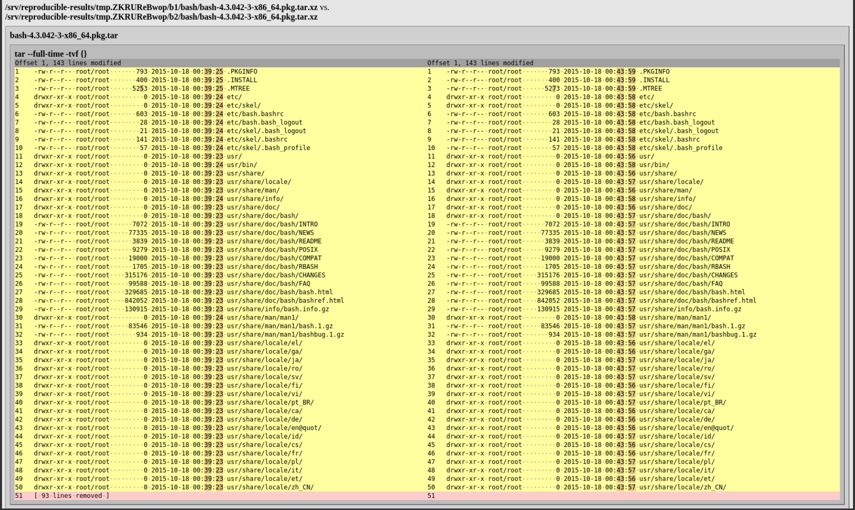
At large scale:

- Automated using Jenkins[2]
- Check the differences with diffoscope[3]
- A lot of help from Lunar and h01ger of the Debian reproducible build team (thanks!)
- Using Debian infrastructure at `https://reproducible.debian.net/archlinux/archlinux.html`

[2] `http://jenkins-ci.org/`

[3] `http://diffoscope.org/`

Diffoscope



/srv/reproducible-results/tmp.ZKRUReBwop/b1/bash/bash-4.3.042-3-x86_64.pkg.tar.xz vs.
/srv/reproducible-results/tmp.ZKRUReBwop/b2/bash/bash-4.3.042-3-x86_64.pkg.tar.xz

bash-4.3.042-3-x86_64.pkg.tar

tar --full-time -tvf {}

```
Offset 1, 143 lines modified
1     -rw-r--r--·root/root······793·2015-10-18·00:39:25·.PKGINFO
2     -rw-r--r--·root/root······400·2015-10-18·00:39:25·.INSTALL
3     -rw-r--r--·root/root·····5253·2015-10-18·00:39:25·.MTREE
4     drwxr-xr-x·root/root········0·2015-10-18·00:39:24·etc/
5     drwxr-xr-x·root/root········0·2015-10-18·00:39:24·etc/skel/
6     -rw-r--r--·root/root······603·2015-10-18·00:39:24·etc/bash.bashrc
7     -rw-r--r--·root/root·······28·2015-10-18·00:39:24·etc/bash.bash_logout
8     -rw-r--r--·root/root·······21·2015-10-18·00:39:24·etc/skel/.bash_logout
9     -rw-r--r--·root/root······141·2015-10-18·00:39:24·etc/skel/.bashrc
10    -rw-r--r--·root/root·······57·2015-10-18·00:39:24·etc/skel/.bash_profile
11    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/
12    drwxr-xr-x·root/root········0·2015-10-18·00:39:24·usr/bin/
13    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/
14    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/
15    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/man/
16    drwxr-xr-x·root/root········0·2015-10-18·00:39:24·usr/share/info/
17    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/doc/
18    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/doc/bash/
19    -rw-r--r--·root/root·····7072·2015-10-18·00:39:23·usr/share/doc/bash/INTRO
20    -rw-r--r--·root/root····77335·2015-10-18·00:39:23·usr/share/doc/bash/NEWS
21    -rw-r--r--·root/root·····3839·2015-10-18·00:39:23·usr/share/doc/bash/README
22    -rw-r--r--·root/root·····9279·2015-10-18·00:39:23·usr/share/doc/bash/POSIX
23    -rw-r--r--·root/root····19000·2015-10-18·00:39:23·usr/share/doc/bash/COMPAT
24    -rw-r--r--·root/root·····1705·2015-10-18·00:39:23·usr/share/doc/bash/RBASH
25    -rw-r--r--·root/root···315176·2015-10-18·00:39:23·usr/share/doc/bash/CHANGES
26    -rw-r--r--·root/root····99588·2015-10-18·00:39:23·usr/share/doc/bash/FAQ
27    -rw-r--r--·root/root···329685·2015-10-18·00:39:23·usr/share/doc/bash/bash.html
28    -rw-r--r--·root/root···842052·2015-10-18·00:39:23·usr/share/doc/bash/bashref.html
29    -rw-r--r--·root/root···130915·2015-10-18·00:39:23·usr/share/info/bash.info.gz
30    drwxr-xr-x·root/root········0·2015-10-18·00:39:24·usr/share/man/man1/
31    -rw-r--r--·root/root····83546·2015-10-18·00:39:23·usr/share/man/man1/bash.1.gz
32    -rw-r--r--·root/root······934·2015-10-18·00:39:23·usr/share/man/man1/bashbug.1.gz
33    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/el/
34    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/ga/
35    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/ja/
36    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/ro/
37    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/sv/
38    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/fi/
39    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/vi/
40    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/pt_BR/
41    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/ca/
42    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/de/
43    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/en@quot/
44    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/id/
45    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/cs/
46    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/fr/
47    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/pl/
48    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/it/
49    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/et/
50    drwxr-xr-x·root/root········0·2015-10-18·00:39:23·usr/share/locale/zh_CN/
51    [·93·lines·removed·]
```

```
Offset 1, 143 lines modified
1     -rw-r--r--·root/root······793·2015-10-18·00:43:59·.PKGINFO
2     -rw-r--r--·root/root······400·2015-10-18·00:43:59·.INSTALL
3     -rw-r--r--·root/root·····5273·2015-10-18·00:43:59·.MTREE
4     drwxr-xr-x·root/root········0·2015-10-18·00:43:58·etc/
5     drwxr-xr-x·root/root········0·2015-10-18·00:43:58·etc/skel/
6     -rw-r--r--·root/root······603·2015-10-18·00:43:58·etc/bash.bashrc
7     -rw-r--r--·root/root·······28·2015-10-18·00:43:58·etc/bash.bash_logout
8     -rw-r--r--·root/root·······21·2015-10-18·00:43:58·etc/skel/.bash_logout
9     -rw-r--r--·root/root······141·2015-10-18·00:43:58·etc/skel/.bashrc
10    -rw-r--r--·root/root·······57·2015-10-18·00:43:58·etc/skel/.bash_profile
11    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/
12    drwxr-xr-x·root/root········0·2015-10-18·00:43:58·usr/bin/
13    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/
14    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/
15    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/man/
16    drwxr-xr-x·root/root········0·2015-10-18·00:43:58·usr/share/info/
17    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/doc/
18    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/doc/bash/
19    -rw-r--r--·root/root·····7072·2015-10-18·00:43:57·usr/share/doc/bash/INTRO
20    -rw-r--r--·root/root····77335·2015-10-18·00:43:57·usr/share/doc/bash/NEWS
21    -rw-r--r--·root/root·····3839·2015-10-18·00:43:57·usr/share/doc/bash/README
22    -rw-r--r--·root/root·····9279·2015-10-18·00:43:57·usr/share/doc/bash/POSIX
23    -rw-r--r--·root/root····19000·2015-10-18·00:43:57·usr/share/doc/bash/COMPAT
24    -rw-r--r--·root/root·····1705·2015-10-18·00:43:57·usr/share/doc/bash/RBASH
25    -rw-r--r--·root/root···315176·2015-10-18·00:43:57·usr/share/doc/bash/CHANGES
26    -rw-r--r--·root/root····99588·2015-10-18·00:43:57·usr/share/doc/bash/FAQ
27    -rw-r--r--·root/root···329685·2015-10-18·00:43:57·usr/share/doc/bash/bash.html
28    -rw-r--r--·root/root···842052·2015-10-18·00:43:57·usr/share/doc/bash/bashref.html
29    -rw-r--r--·root/root···130915·2015-10-18·00:43:57·usr/share/info/bash.info.gz
30    drwxr-xr-x·root/root········0·2015-10-18·00:43:58·usr/share/man/man1/
31    -rw-r--r--·root/root····83546·2015-10-18·00:43:57·usr/share/man/man1/bash.1.gz
32    -rw-r--r--·root/root······934·2015-10-18·00:43:57·usr/share/man/man1/bashbug.1.gz
33    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/el/
34    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/ga/
35    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/ja/
36    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/ro/
37    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/sv/
38    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/fi/
39    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/vi/
40    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/pt_BR/
41    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/ca/
42    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/de/
43    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/en@quot/
44    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/id/
45    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/cs/
46    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/fr/
47    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/pl/
48    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/it/
49    drwxr-xr-x·root/root········0·2015-10-18·00:43:56·usr/share/locale/et/
50    drwxr-xr-x·root/root········0·2015-10-18·00:43:57·usr/share/locale/zh_CN/
51
```

Is it really that easy?

Is it really that easy?

That's the theory, but you know the difference between theory and practice, right?

- Timestamps
- Paths
- Locale / Timezone
- CPU type
- UID / GID
- Randomness
- Build chain

Fixing the reproducible build issues

A lot of fixes in our toolchain:

- Timestamps in static archives (#45935, –enable-deterministic-archive in binutils)
- Timestamps in packages
- Build chain versions and build options are added to the packages in .BUILDINFO[4]
- ...

[4] `https://lists.archlinux.org/pipermail/pacman-dev/2015-October/020357.html`

Fixing the reproducible build issues

Ideally, we would like to see SOURCE_DATE_EPOCH specification[5] being adopted:

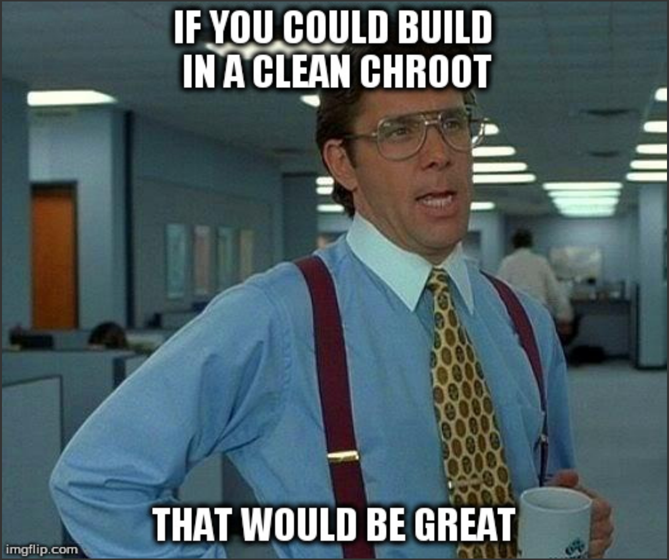
- A UNIX timestamp.
- The value SHOULD be set to the time of the last modification time of the source, incorporating any packaging-specific modifications. For example, in Debian, the timestamp of the latest entry in debian/changelog.
- Upstream build processes MUST use this variable for embedded timestamps in place of the "current" date and time.

[5] `https://reproducible-builds.org/specs/source-date-epoch/`

Fixing the reproducible build issues

- If you are developing a software, please do not includes the build time, the builder uid/gid..
- Or at least include an option to get rid of that, like –enable-reproducible
- Good news is, we are not alone working on that, and a lot of fixes are pushed upstream
- If you are a Trusted User or a Developer, please build in a clean chroot with makechrootpkg

Fixing the reproducible build issues



Final words about reproducible builds

- As always with security, this is a process, not a product
- Reproducible builds are too valuable to neglect
- Respect the KISS philosophy

Hardening Arch

Why harden?

- Not-so-breaking news: there are vulnerabilities in Arch
- We are good at upgrading, so known vulnerabilities are patched fast
- Still, we depend heavily on upstream
- What about unknown vulnerabilities?
- Raising the exploitability bar

What kind of hardening?

What kind of hardening?

- Hardening packages at build time
- Protecting pacman's database

I will not talk about:

- Kernel Hardening with grsecurity: linux-grsec and paxd, maintained by Daniel Micay
- Configuration hardening: use the wiki[6]

[6] `https://wiki.archlinux.org/index.php/Security`

Hardening Arch: binaries

Default build options

Arch does enable some interesting features by default:

- CPPFLAGS=”-D_FORTIFY_SOURCE=2”, buffer overflow prevention
- CFLAGS=”[...] -fstack-protector-strong” stack overflow prevention
- LDFLAGS=”-Wl,-O1,–sort-common,–as-needed,-z,relro” read-only relocation (partial)

RELRO

- Prevent some parts of ELF binaries (non-PLT GOT, dtors, ctors) from being writable
- With “full” RELRO, even the PLT GOT is computed at load time and is not writable afterwards. The cost is minimal for daemons

Position-Independent Executable

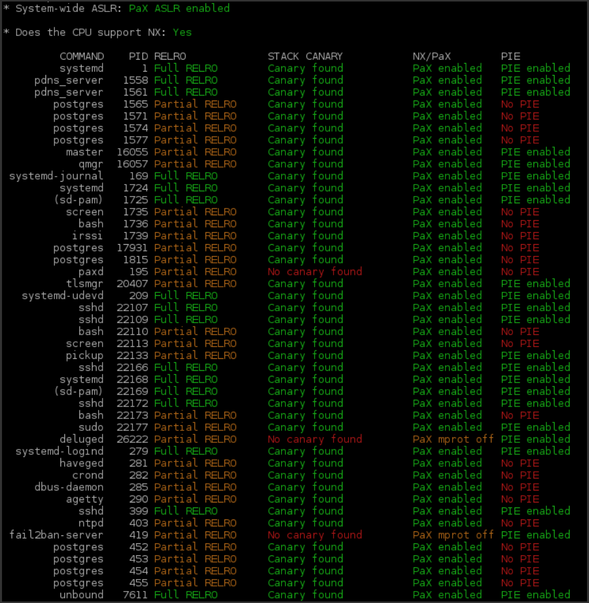
- Thanks to No-eXecute (NX)/ PaX, you can't just put your shellcode in memory and execute it, you have to use Return-Oriented Programming (ROP), exploiting already existing gadgets
- With recent kernels, PIC code from libraries is loaded at a random location, thanks to Address space layout randomization (ASLR)
- This makes it harder to find gadgets in it, but the code of the executable itself is predictable without Position-Independent Executables (PIE)
- PIE cost is now very low on x86_64, since gcc's 5.1 new register allocation algorithm
- We need a gcc switch to make PIE the default: –enable-default-pie (in gcc 6.0, not backported to 5.x yet)

Hardening: Try harder

Hardening selected packages:

- Time-consuming, fail-open
- PIE, full-RELRO, non-executable stack for selected packages, ie network daemons, browsers (Firefox, Chromium)
- Need upstream support to do it right (recently pushed upstream to NSD, Unbound)

Using checksec to verify the results



```
* System-wide ASLR: PaX ASLR enabled

* Does the CPU support NX: Yes

         COMMAND    PID RELRO             STACK CANARY           NX/PaX        PIE
         systemd      1 Full RELRO        Canary found           PaX enabled   PIE enabled
     pdns_server   1558 Full RELRO        Canary found           PaX enabled   PIE enabled
     pdns_server   1561 Full RELRO        Canary found           PaX enabled   PIE enabled
        postgres   1565 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres   1571 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres   1574 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres   1577 Partial RELRO     Canary found           PaX enabled   No PIE
          master  16055 Partial RELRO     Canary found           PaX enabled   PIE enabled
            qmgr  16057 Partial RELRO     Canary found           PaX enabled   PIE enabled
 systemd-journal    169 Full RELRO        Canary found           PaX enabled   PIE enabled
         systemd   1724 Full RELRO        Canary found           PaX enabled   PIE enabled
        (sd-pam)   1725 Full RELRO        Canary found           PaX enabled   PIE enabled
          screen   1735 Partial RELRO     Canary found           PaX enabled   No PIE
            bash   1736 Partial RELRO     Canary found           PaX enabled   No PIE
           irssi   1739 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres  17931 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres   1815 Partial RELRO     Canary found           PaX enabled   No PIE
            paxd    195 Partial RELRO     No canary found        PaX enabled   No PIE
          tlsmgr  20407 Partial RELRO     Canary found           PaX enabled   PIE enabled
   systemd-udevd    209 Full RELRO        Canary found           PaX enabled   PIE enabled
            sshd  22107 Full RELRO        Canary found           PaX enabled   PIE enabled
            sshd  22109 Full RELRO        Canary found           PaX enabled   PIE enabled
            bash  22110 Partial RELRO     Canary found           PaX enabled   No PIE
          screen  22113 Partial RELRO     Canary found           PaX enabled   No PIE
          pickup  22133 Partial RELRO     Canary found           PaX enabled   PIE enabled
            sshd  22166 Full RELRO        Canary found           PaX enabled   PIE enabled
         systemd  22168 Full RELRO        Canary found           PaX enabled   PIE enabled
        (sd-pam)  22169 Full RELRO        Canary found           PaX enabled   PIE enabled
            sshd  22172 Full RELRO        Canary found           PaX enabled   PIE enabled
            bash  22173 Partial RELRO     Canary found           PaX enabled   No PIE
            sudo  22177 Partial RELRO     Canary found           PaX enabled   PIE enabled
         deluged  26222 Partial RELRO     No canary found        PaX mprot off PIE enabled
  systemd-logind    279 Full RELRO        Canary found           PaX enabled   PIE enabled
         haveged    281 Partial RELRO     Canary found           PaX enabled   No PIE
           crond    282 Partial RELRO     Canary found           PaX enabled   No PIE
     dbus-daemon    285 Partial RELRO     Canary found           PaX enabled   No PIE
          agetty    290 Partial RELRO     Canary found           PaX enabled   No PIE
            sshd    399 Full RELRO        Canary found           PaX enabled   PIE enabled
            ntpd    403 Partial RELRO     Canary found           PaX enabled   No PIE
 fail2ban-server    419 Partial RELRO     No canary found        PaX mprot off PIE enabled
        postgres    452 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres    453 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres    454 Partial RELRO     Canary found           PaX enabled   No PIE
        postgres    455 Partial RELRO     Canary found           PaX enabled   No PIE
         unbound   7611 Full RELRO        Canary found           PaX enabled   PIE enabled
```

Hardening Arch: signing pacman's database

Signing pacman's database

Right now:

- Packages are signed using the packager's PGP key
- Databases are not signed

What is in the database?

- Actually one database per repository: core, extra, community, ...
- Tarball of files, one file per package
- Package file contains meta-data: name, version, description, size, dependencies, PGP signature..

What is in the database?

```
%FILENAME%
getdns-0.3.3-1-x86_64.pkg.tar.xz

%NAME%
getdns

%VERSION%
0.3.3-1

%DESC%
A modern asynchronous DNS API

%PGPSIG%
[...]

%URL%
http://getdnsapi.net/

%ARCH%
x86_64

%BUILDDATE%
1443175743

%PACKAGER%
Remi Gacogne <rgacogne-arch at coredump dot fr>

%DEPENDS%
libev
libevent
libidn
libuv
unbound
```

What's wrong?

While packages are signed, database is not, so a:

- Rogue mirror
- Man-on-the-middle
- Man-on-the-side

can:

- Hide packages
- Prevent upgrade

by altering the database.

Proposed design

Separate PGP keyring for signing the database:

- Database key is not allowed to sign packages
- Packagers are not allowed to sign the database
- Master database keys stay offline
- Database signing key is online, not readable by packagers, used by repo-add to sign the database
- Can be revoked if needed
- At worst, In case of compromission, we are back to where we are today

Conclusion

Help is always welcome!

There is always some interesting projects to work on, for every skill level, and nobody expects you to commit a lot of time.

- https://wiki.archlinux.org/index.php/Arch_CVE_Monitoring_Team
- #archlinux-security on Freenode
- arch-security@archlinux.org
- If you are willing to help but don't know where to begin, please mail me: rgacogne@archlinux.org

Thank you! / Questions?

Powered by LaTeX, based on a theme by kaszkowiak.eu