ArchLinux Security Team Genesis

Robin Marsollier

November 10, 2015

$ whoami

- Robin Marsollier
- Security Analyst (forensics, incident response etc.) at Conix Security
- Long time Arch user

Began as a personal project

- To secure my laptop
- To learn

How to harden my Arch?

- Apply all the usual recommendations you can find online
  - Arch wiki great on this matter
- Follow vulnerabilities/exploits news

How to harden my Arch (next step)?

- But soon, the best way to get more security was to:
  - Secure the whole distribution
  - Not just my laptop
- By ensuring patch were applied soon

August, 2013

- When everything began
- Beginning of me trying to follow the CVEs
- Trying to make them patched too

Starting point

- Very few bugs mentionning CVE in the FlySpray
- No explicit policy about patching vulnerabilities
- Patching was done by devs/TUs only when they were aware of vulnerabilities

- *This was a cultural shift for ArchLinux*

Howto?

- Strategy:
  - Make things better, not perfect
  - Not waste my time
  - Skip some packages
  - Skip aur (nearly impossible to manage)

Howto?

- Means :
  - Try to be as assisting as possible with devs/TUs
  - Flag out of date or opening bugs and no more
  - Just making devs/TUs aware of CVEs was a significant progress

Tracing vulns

- As I was alone to do this work
  - A flat file on my desktop was enough

glibc	CVE-2013-4332	11/09/2013	core	16/09/2013	4 days	
lightdm	CVE-2013-4331	11/09/2013	community	13/09/2013	2 days	
wordpress	CVE-2013-4339 CVE-2013-4340	12/09/2013	community	13/01/2013	1 day	
openjpeg	CVE-2013-4289 CVE-2013-4290	12/09/2013	extra	no patches available		
gnupg	CVE-2013-4351	13/09/2013	core	05/10/2013	21 days	not critical
icedtea-web	CVE-2013-4349	16/09/2013	extra	16/09/2008	0 day	(CVE-2012-4540 reintroduced in 1.4)
vino	CVE-2013-5745	16/09/2013	extra	23/09/2013	7 days	
glibc	CVE-2013-4357	17/09/2013	core			known since 2011
davfs2	CVE-2013-4362	18/09/2013	extra	13/01/2014		~~~bug FS#37002~~~
polkit	CVE-2013-4288	18/09/2013	extra	19/09/2013	1 day	
libvirt	CVE-2013-4311	18/09/2013	community	25/09/2013	7 days	
spice-gtk	CVE-2013-4324	18/09/2013	community	23/09/2013	5 days	
hplip	CVE-2013-4325	18/09/2013	extra	13/10/2013	25 days	~~~bug FS#37168~~~
rtkit	CVE-2013-4326	18/09/2013	extra	02/10/2013	14 days	~~~bug FS#37169~~~
systemd	CVE-2013-4327	18/09/2013	core	21/09/2013	3 days	
systemd	CVE-2013-4391 to CVE-2013-4394	01/10/2013	core	02/10/2013	1 day	

Tools

- None
  - Some reuse of tools of other distributions

Security Advisories

- None issued
  - Very time consuming to do

March 2014

- New work
  - Less spare time
  - No time for ArchLinux at all

Stepping down

- Mailing Allan to make devs aware of it
- Creation of the ArchLinux-security mailing-list
- Creation of #archlinux-security on Freenode
- Official creation of a team dedicated to this kind of issues (anyone left today?)

Stepping down

- Writing wiki pages on the subject
  - Where to find information?
  - How to notify devs/TUs?
    - Etc.
- Passing on the knowledge

8 months of CVE monitoring

- More than 200 CVEs taken care of
  - Worst response time was ~60 days
- 53 bugs open
  - All closed now (hopefully :)

Fondation stone was put in place

- Devs/TUs aware of CVEs and willing to correct them :)
- A handfull of people interested in continuing this work

Questions?

- Now, the next chapter of this story, Rémi's talk

- Mail : *r.b.n@riseup.net*
- GPG : 0xBC28268A7B91EEE9
- Fingerprint : 5FDE 8B30 FEEB 3709 D609 BE25 BC28 268A 7B91 EEE9
- Twitteur : *@rbnctl*
- IRC : RbN_ (freenode, OFTC)