The work of security teams

Mateusz Kocielski

shm@NetBSD.org

LogicalTrust

pkgsrccon
Kraków, July 02, 2016

THANKS

kamil@ & co-organizers

THANKS

kamil@ & co-organizers

applause.wav

whoami(1)

- pentester at LogicalTrust
- open source committer:
  - NetBSD - libsaslc(3), bozohttpd(8), hacking random things & secteam member
  - PHP - bug finding & fixing
- security:
  - PHP - CVE-2010-1868, CVE-2010-1917, CVE-2010-4150, CVE-2010-4156, CVE-2011-1938, CVE-2016-5768, ...
  - stunnel - CVE-2013-1762
  - OpenSSH - CVE-2011-0539
  - Apache - CVE-2014-0117, CVE-2014-0226
  - FreeBSD - CVE-2015-1414
  - NetBSD - CVE-2015-8212, ...
  - ...

NetBSD & Security

- exploit mitigations
  - ASLR
  - PaX
  - SSP
  - FORTIFY
  - kernel based NULL pointer dereferences
- blacklistd(8)
- veriexec(8)
- ...
- see security(7)
- it's clear we all care about security

Motivation behind this talk

- what's going on behind security-team@
- what we do
- what need to be done to issue a security report
- what can be done better

security-related groups in the NetBSD

- security-alert@ - Security Alert Team
  - An emergency contact address for notifying the NetBSD project of security issues. Less of a formal 'group' than security-officer@.
- security-team@ - Security Team
  - Responsible for handling security issue resolution and announcements.
- security-officer@ - Security-Officer
  - Responsible for assisting to resolve security issues and preparing announcements.
- pkgsrc-security@ - pkgsrc Security Team
  - Responsible for handling pkgsrc security issues.

security-team@ - what you do?

- we try to keep the NetBSD code safe
- pressure of time
- we assist in
  - cooperating with 3rd parties to exchange information on issues
  - evaluating potential vulnerabilities
  - preparing patches
  - preparing advisories
  - cooperating with other devs to keep our codebase safe
- `http://www.netbsd.org/support/security/advisory.html`
- 252 advisories since 1998
- whole bug cycle usually takes from few hours to days

security-team@ - advisories - stats per year

2000. 17
2001. 18
2002. 27
2003. 18
2004. 10
2005. 13
2006. 26
2007. 7
2008. 15
2009. 13
2010. 13
2011. 9
2012. 4
2013. 13
2014. 15
2015. 12
2016. 5

security-team@ - cooperating with 3rd parties/devs

- cooperating with 3rd parties
  - "Hey NetBSD, there's a bug in XXX"
  - receiving confidential information about bugs in 3rd party software
  - coordinated disclosure (usually information is embargoed until someday)
  - "Hey 3rd party software, there's a bug in XXX"
  - communication usually bases on trust $\rightarrow$ we have to keep the information in confidential
- "Hey TCP-stack wizard, there's a nasty bug in TCP implementation, may I ask you to help us fix that?"

security-team@ - evaluating potential vulnerabilities

- evaluating bug impact
- local DoS that can be triggered by privileged user $\neq$ remote code execution due to bug in kernel
- trying to figure out the root cause
- looking for solutions and workarounds
- trying to figure out technical implications

security-team@ - preparing patches

- working with random parts of the code
- security related patches should be crafted with carefulness
  - PHP fixed few bugs... and introduced other vulnerabilities :)
- arrange pull-ups to supported branches
  - coordinate devs
- need to deal with different versions of 3rd party software
  - like unmaintained OpenSSL 0.9.x in NetBSD 5.x

security-team@ - preparing advisory

- provide information on
  - vulnerable branches
  - technical details
  - solutions and workarounds
    - how to deal with bug
    - how to fix from autobuilds
    - how to fix from source
- requires writing in English...
- usually painful process (at least for me :))

security-team@ - what can be done better?

- minimize time frame between notification about the bug and advisory publication
- binary patches (see FreeBSD's freebsd-update(1))
- Security Notices
- proactive NetBSD code audits

Reporting a security issue

- contact security-alert@ (remember about PGP)
- send-pr(1)
  - if you suspect the bug is important, then use security-alert@
- provide as many details as you can
- root case/patches more than welcome

How you can help?

- fix bugs from coverity scans
- notify us if you see potential hole in the NetBSD
- audit the NetBSD code
- try to provide as many details as you can
- **we need fresh blood** - join us to make the NetBSD safer place for you and me

my projects - fuzzing + rump

Become a hero:

- I'm fuzzing various parts of the NetBSD using rump(7)
- now I'm focused on network stack
- Address Sanitizer (other sanitizers?)
- if you want to join me, drop me a line → shm@NetBSD.org
- think about your master thesis/research/fun
- test my SMEP/SMAP implementation

Q&A