Security Vulnerability Reporting

Kernel Summit 2013
0-day slides!

keescook@{chromium.org,google.com}
kees@outflux.net

Goals

- Get fix to end users
- Identify severity
- Reduce window of public exposure
- Help maintainers/distros with identification

What's the process?

- Don't know if it's a security issue? Ask!

  security@kernel.org

  linux-distros@vs.openwall.org (“Subject: [vs] ...”)
- If it's high priority, attempt will be made to handle it with distros in a coordinated fashion
- If it's low priority, may be better to take it to a public devel list (e.g. lkml, net-dev, etc)
- Let other people know when public

  oss-security@lists.openwall.org

Recommended Tags

- Request it be included in the stable tree:

  Cc: stable@vger.kernel.org

- Help stable maintainers (and others) figure out if they are vulnerable by identifying which commit introduced the flaw:

  Fixes: 12-char-SHA (“TITLE”)

Nice to have: CVE

- Get a CVE assigned (try to include it in the commit message)
  - If you work for a vendor that is a “CVE Naming Authority”, you can get your own, otherwise, emailing oss-security should cause someone to assign you one.
- If not, someone may get one assigned for your change anyway at some mysterious point in the future.

Didn't realize it was a security fix?

- That's okay!
  - Ask Greg to include it in stable

    gregkh@linuxfoundation.org
  - Let oss-security know about it (will trigger CVE)

Questions?

keescook@{chromium.org,google.com}
kees@outflux.net