Sysadministrivia

Linux, Lagers, and Late Nights

S0E13: "Better Late than Never"

Posted 2015-08-31 08:25
Modified 2018-12-03 03:35
Comments 0

Navigation

Previous Episode	Next Episode
S0E12: "It Hurts when IP"	S0E14: "A Failed Experiment"

Log

Recorded (UTC)	Aired (UTC)	Editor
2015-07-31 04:55:19	2015-08-31 08:25:45	MOQ

Verification

Format	SHA256	GPG	Audio File
MP3	`87575aea34439873404702a49bd038f1c376e0596b51d0ce44206ce046d7189c`	click	click
OGG	`ed06b642e6c190f4a89af3c189636a133f7a7da346d4820517c5b0546156d43a`	click	click

Quicklisten:

We discuss an Android vulnerability, GNU/Linux malware, OpenSSH v7.x, more NSA nonsense, a case study of extreme-low-latency networks, BSD comparison, and some home NAS software.

- Notes
- Errata
- Music

Notes

- The Stagefright vulnerability (CVEs: CVE-2015-1538, CVE-2015-1539, CVE-2015-3827, CVE-2015-3826, CVE-2015-3828, CVE-2015-3824, CVE-2015-3829). You can find more information and a PoC here.
  - The iOS thing
  - I ran the Stagefright detector app and it seems CyanogenMod (at least the nightlies, as of 08.29.2015) is not vulnerable.
  - Speaking of Android/CyanogenMod and security, you may want to check out Copperhead OS, a hardened and privacy-focused fork of CyanogenMod.
- @MalwareMustDie is awesome. They found this malware, and present an awesome case study on it.
  - Jthan suggests joining a mailing list. Here are some good ones. Mitre, OSS-Sec, Full Disclosure, etc.- a lot of really good lists are available for subscription at SecLists.org (maintained by the Nmap project maintainer/author, Fyodor).
- Not only has OpenSSH 6.9 released, but all the way up to 7.1 has as well!
  - You can read the changelog document we reference here...
  - But you can read the changelog for 7.1 here.
  - The weak DH thing (“Logjam”). We talk about it in S0E8.
  - We are mirroring this article. Very useful for securing SSH down.
- XKEYSCORE
  - Ignore my entire rant about Stingrays. See Errata.
- Cloudflare’s 10Gbps thing
- BSD’s:
  - FreeBSD
  - NetBSD
  - OpenBSD
  - DragonFlyBSD
  - PC-BSD
  - Junos OS
  - OpenBSD is responsible for starting/maintaining the following projects:
    - OpenSSH
    - OpenNTPD
    - OpenBGPD
    - OpenSMTPD
    - pf
    - CARP
    - LibreSSL
  - FreeSBIE is still “around”, sort of. There’s been no release since v2.0.1, on February 10, 2007.
  - pfSense we mentioned in S0E10.

    - And yes, there is indeed BSD code in older versions of Windows.
    - PonyOS…
    - MenuetOS is the OS written entirely in Assembly (“ASM”).
        - There seem to be other, similar projects however.
    - Got the name wrong, but I reference TempleOS (see errata).
- FreeNAS
    - OwnCloud

Errata

I am terribly sorry for the delay with this. We tried to use a new editor. It didn’t work out per the normal schedule. That plus FOSSCON and our entire schedule got out of whack. We’ll try harder to release per our normal schedule (2x month/every other week).

- When I’m giving the topic summary, I say “OwnClown” at first instead of “OwnCloud”. Hah, whoops.
- Blowfish-CBC has some issues.
- I suggest the *possibility* of the Snowden leaks being a false flag. I called it a “black flag”, oops.
    - Jthan means intelligent, not intelligible.
    - Whooooops. I totally was saying Stingrays when I was thinking of the GT200 / ADE651 / Sniffex / etc. (you’d be amazed at how many of these there are). But Stingrays are real, and “work”- but they’re somewhat easy to detect.
- The plural terminology for Unix is generally considered one of Unixes, Unices, or Unixen
    - *pf* is short for *packet filter*, not *packet firewall*.
    - I said ArkOS. I meant TempleOS.

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Disco Medusae	Kevin MacLeod	click	CC-BY 3.0
Outro	Decisions	Kevin MacLeod	click	CC-BY 3.0

(All music is royalty-free, properly licensed for use, used under fair use, or public domain.)

Author r00t^2
Categories (Pilot Season)

Comments

There are currently no comments on this article.