Sysadministrivia

Linux, Lagers, and Late Nights

S2E19: "Patching the KRACKs in the (Fire)Wall"

Posted 2017-11-06 04:59
Modified 2017-11-11 00:46
Comments 0

Navigation

Previous Episode	Next Episode
S2E18: "Dueling Banditos"	S2E20: "The Shell Game"

Log

Recorded (UTC)	Aired (UTC)	Editor
2017-10-26 02:36:27	2017-11-06 02:25:06	"Edita"

Verification

Format	SHA256	GPG	Audio File
MP3	`b0358ec555faa290b0ddeeb7c18c586a1d204566f21498c85530d79e3cd611a9`	click	click
OGG	`7e754aa9e2a1cbba03e153089e96637e48acbc49080934fd39e8cedc1726d502`	click	click

Quicklisten:

In which we talk about KRACK (and ROCA, the RSA flaw in some TPM chips), and how to perhaps move forward/past the “unpatchable/limited patching in prod” scenario.

- News
- Notes
- Sysbadministration Award
- Errata
- Music

News

- KRACK, a vulnerability against WPA2 encryption/handshaking, has dropped
  - CVEs:
    - CVE-2017-13077
    - CVE-2017-13078
    - CVE-2017-13079
    - CVE-2017-13080
    - CVE-2017-13081
    - CVE-2017-13082
    - CVE-2017-13084
    - CVE-2017-13086
    - CVE-2017-13087
    - CVE-2017-13088

- ROCA, an RSA flaw in Infineon TPM chips
  - CVE-2017-15361

- Dell lost control of a customer support domain for a month
- More than half of emails worldwide are opened in a mobile environment
- NotPetya is back as Bad Rabbit
- Kaspersky released a full incident report of the NSA leak
  - We forgot to mention this, but they also opened source code to independent review

Notes

Starts at **12m46s**.

I was drinking the Bulleit 10-year bourbon. Paden was drinking Miller Lite and Glenlivet Founder’s Reserve. Jthan was drinking Woodford Reserve’s Distiller’s Select (he didn’t specify which).

- Dispelling KRACK rumours

    - No, WPA3 isn't really necessary; it's possible to patch
    - The attack surface, while affecting a vast majority of devices, only really affects GNU/Linux the most (including Android). wpa_supplicant and hostapd are patched, but your distro may not have incorporated it yet (as of recording; as of *release*, however, I'd imagine most/all distro's versions should be patched).
        - Android 6.0 is fucked, and good luck getting an OTA update from your vendor. You're better off with LineageOS since it's already fixed there (we talk about alternate Android firmware in S0E3, and LineageOS specifically in S2E1 and S2E2).
            - Luckily, however, for the future – it seems that direct updates for Android are coming. It probably won't do you much good for current vendor firmware, though.

    - The attack is more useful combined with other attacks such as rogue/spoofed APs. An end-to-end encrypted connection that has integrity verification (such as a strong VPN) helps thwart them. I also mention HTTPS Everywhere (but that will ONLY protect web traffic, and only opportunistically). If you need a provider, you may want to consider the company I work for.

- How to address the "patching window/patching stable systems" problem **(33m43s)**
    - It's important to not challenge the pre-scheduled maintenance/patch windows, because otherwise they'll keep being pushed off/delayed, which can also cause issues with standards and compliance and such.
    - Standardized hardware across your fleet can help **a lot**.
    - Patch/change management does have valid application, presently – because patches/changes **can** break things. It's likely, however, that you don't need it because you aren't offering services that are this critical.
    - We talk about Dev/Testing/Staging/Prod platforming in more detail in S2E2.
    - Paden mentions The Phoenix Project
        - But note that it's probably not always 100% applicable; these are for large-scale corporate environments.

    - Try to address the issue with alternatives – firewall rules, etc.
    - Airgapping helps…
    - Automated change management software also helps.
    - Make sure you're validating your patching.
    - If you have something that can't be patched but needs to be, it might be time for a different vendor/product/solution.
    - In terms of locking down implementations that can't be patched, outbound traffic rules are incredibly useful and underestimated.
    - If you have any other ideas, please be sure to contact us!

Sysbadministration Award

In this segment, we highlight system administration mistakes. Think of them as the IT equivalent of the Darwin Awards. **(58m21s)**

The DOJ appears to have subpoena'd Twitter regarding five individuals over emoji usage. Because they used these emoji to interact with one particular person.

Errata

- Jthan never sent me a photo of the train tracks. :(
- Paden references /r/homelab.
- We already got some suggestions in on creative ways of addressing hard-to-patch systems!
    - **raindev** in our IRC channel said *"I use iptables to have VPN-only internet connection."* Great idea! We'd probably implement this by DROPping **all** outbound traffic on the primary/WAN interface of the client/machine in question, except for the specific port and protocol to the VPN gateway/peer (because it needs to establish initial connection) and then to a wide ALLOW on the VPN subnet. I haven't tested this, but if you have the default route set to the VPN gateway this has the added benefit of doing a sort of "Dead Man's Switch" if your VPN should fail to connect. However, in a corporate environment, it's likely you're only tunneling certain data through that VPN (i.e. cross-VLAN or the like). It also would let you centralize all traffic more easily for analysis. Definitely a lot of flexibility there. Thanks, raindev!

Music

Music Credits

Track	Title	Artist	Link	Copyright/License
Intro	Persistence [With Beat]	Rafael Archangel	click	CC0 1.0
Outro	Good Grief	Ryan Little	click	CC-BY 4.0

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

Author r00t^2
Categories Season Two

Comments

There are currently no comments on this article.