This talk is not about LTE vulnerabilities

No cables

Why isn’t it working?
Scared Poopless – LTE and *your* laptop

Disclaimer:
During the slides you will be exposed to hacker stock photos from the internet.
Thank you!

Goldy
aSmig
@octosavvi
Intel Security would like to acknowledge and thank the Huawei PSIRT team for their responsiveness and cooperation on this issue.

- CVE-2015-5367: Insecure Linux Image in Firmware
- CVE-2015-5368: Insecure Firmware Update Authentication

DEMO
What did I just see?
This is not a Dell problem
Remember kids!
This is why you should do
secure firmware updates

NEVER FORGET

Adam Caudill
Brandon Wilson
Who are we?

@jessemichael
@laplinker
Background

- Internal LTE/3G modems and who uses them?
• Internal LTE/3G modems and who uses them?
• Business class devices

I think I have an idea!
• Internal LTE/3G modems and who uses them?
• Business class devices
• How is it plugged in anyway?
• Internal LTE/3G modems and who uses them?
• Business class devices
• How is it plugged in anyway?
• Internal LTE/3G modems and who uses them?
• Business class devices
• How is it plugged in anyway?

PCIe ×2, SATA, USB 2.0 and 3.0, Audio, PCM, IUM, SSIC and I2C

I forgot mac’s don’t have a CD drive anymore
• Internal LTE/3G modems and who uses them?
• Business class devices
• How is it plugged in anyway?
• USB?!

Crap! I just stabbed my USB thumb drive!
• Internal LTE/3G modems and who uses them?
• Business class devices
• How is it plugged in?
• USB?!
• Why hack this device anyway?
Background

- Internal LTE/3G modems and who uses them?
  - Business class devices
- How is it plugged in?
  - USB?!
- Why hack this device anyway?
  - Module available worldwide
  - It’s plugged in [INSIDE] your laptop/tablet
• Software
• Firmware
• Hardware
• Software
• Windows utility for firmware updates
• Firmware
• Hardware
• Software
  • Windows utility for firmware updates
• Firmware
  • Packed in software utility
• Hardware
What do you mean you can see my face?

- Software
  - Windows utility for firmware updates
- Firmware
  - Strings is useful
- Hardware
• Software
  • Windows utility for firmware updates
• Firmware
  • Strings is useful
• Hardware
  • Test pads?
• Software
  • Windows utility for firmware updates
• Firmware
  • Strings is useful
• Hardware
  • Test pads?
Got root shell!

```bash
INIT: Id "rb" respawnning too fast: disabled for 5 minutes
OpenEmbedded Linux 9615-cdp ttyHSL0
msm 20130621 9615-cdp ttyHSL0
9615-cdp login: root
Password:
login[317]: root login on 'ttyHSL0'
root@9615-cdp:~# uname -a
Linux 9615-cdp 3.0.21+ #1 PREEMPT Fri Jun 21 17:55:56 CST 2013 armv7l GNU/Linux
root@9615-cdp:~#```
Happy shell dance
Obligatory success meme
• We have root shell on a Linux run, independent device inside the physical platform.
Firmware structure

92-byte file header

98-byte object header

DWORD at offset 0x5E: object block size

WORD at offset 0x5C: object header CRC

DWORD at offset 0x18: object data size

Data block 0

WORD at offset 0x00: data block 0 CRC

WORD at offset 0x02: data block 1 CRC

WORD at offset N*2: data block N CRC

Data block 1

Data block N

Data size relationships

CRC value/data correspondence

Creeper hacker
Updater patch

- Updater checks CRC
- Updater calculates the correct CRC and compares to the one in the firmware image
- Modify updater code to save correct CRC in image instead of comparing it
- Total op code change = 6 (not including NOP padding)
Summary

• We had a cool demo!
• There is such a thing as an insider threat, literally.
• Secure your firmware updates.
Questions?