Linux Firmware Database

https://lfwdb.com/

Hello, My Name Is Nick

- Threat Researcher at HPE Aruba Networking
- Firmware Security Researcher
- SecDSM Member

What is “linux-firmware”?

- Git repository hosted at: https://git.kernel.org/pub/scm/linux/kernel/git/firmware/linux-firmware.git/
- Contains proprietary firmware blobs that are loaded into peripheral DRAM for the attached device to function properly
- Things like WiFi adapter firmware, Ethernet adapter firmware, PCI card firmware, etc
- Maintained by the Linux Community (Read: Redhat)
- Included in most Linux Distributions

What is LFWDB

- Hosted at https://lfwdb.com/
- Source code at: https://github.com/nstarke/linux-firmware-db
- Data is hosted in the repository, along with all the scripts necessary for building the dataset.

Why did I build LFWDB?

- Easy reference for linux-firmware metadata
- Raise awareness for these proprietary blobs
- Gain insight into how they work?

How does LFWDB Work?

- 3-pass process
  - Run CPU_REC, output to text - takes about 3 hours @ ~3000 blobs
  - Run GNU File, generate SHA256sum, output to CSV - takes about 30 minutes @ ~3000 lines of text
  - Convert CSV to JSON - takes less than a second @ ~3000 lines of csv
- Once data is in JSON format:
  - run disassembly (if possible)
  - Commit data to repository
  - Push repo to remote
- Github actions handles deployment

Web Interface at https://lfwdb.com/

LFWDB has a web interface meant for general consumption.

VueJS based

Sortable

Filterable

Deployment via Github actions results in web interface update

Data directory is publicly accessible and can be used as a REST API

Disassembly

- Hit and miss
- Only works for certain CPU Architectures
- Uses Radare2 for disassembly
- Automated disassembly as part of the data build process.

Where does the data build run?

On a NUC in my basement

- 16 logical cores
- 64 GB RAM
- 256 GB disk space - NVMe
- 1GB fiber uplink.

Why self host?

- Cloud is expensive and slow.

Insights

- Lots of the blobs are encrypted
- Some are more encrypted than others
- Some vendors are more likely to encrypt

Encrypted?

There is also an encrypted zip file for two firmware files.

- Attempted to crack the zip file - no success
- Attempted to extract the password by physically dumping peripheral ROM - no success
- Attempted to dump EFI/BIOS Option ROM from Linux - no success

Question?

Thank you!

Contact:

“The Reason” on SecDSM Discord.

See https://discord.com/invite/aqcDKzVYw3 to get signed up!

https://starkeblog.com/

https://nstarke.bandcamp.com/

https://www.youtube.com/channel/UCQGtCEVsTBtzcNYRqjduwtQ