SMARTWATCH PENTEST

Garmin VivoActive 3 Music

Anouk Brondijk

Contents

1. Management Summary

The security of VivoActive 3 Music smartwatch, made by Garmin, is very well put together. No critical security flaws could be found.

2. Vivoactive 3 Smartwatch

VivoActive 3 Music is a SmartWatch from Garmin. It’s mostly focused on health and sports, but cam also control music on your phone. It also shows calls and messages. It has up to 3 GB of storage to store music locally.

It connects to your phone via Bluetooth, but it can also connect to wifi with the help of an app on your phone, called Garmin Connect. With the app, you can see what’s being measured with the smartwatch, and you can set your age, likes, and health goals like steps.

2.1 Research question

The watch itself will be tested, not the app or the phone. The watch will be analyzed, how it works, what it runs on, and if there’s anything that can be taken advantage of.

2.2 Scope

The watch is in the scope, but not the smartphone or the app. The only change to the watch is being connected to the app on the android phone, so it will have features like calls, downloads, and wifi.

3. Findings

3.1 Approach

To test the watch, Nmap and Wireshark were used to scan ports and the network for packets; further, there was more research done to the OS that the watch used.

3.1.1 General

The first thing that was tested for was reconnaissance. Nmap was used to find any open ports. There were none open, however. There was also an attempt to scan for Bluetooth; however, after extensive research, it was determined it wouldn't be possible to do. I did scan with Wireshark to see if I could find any packets from there, and I did find some, but the problem was that the packets didn't really contain anything. They aren't sent to an IP address, but to the wifi-MAC of the watch itself that it uses instead.

To try something else, the next step is looking into the OS it uses, the Garmin OS. Searching the CVE site, however, offered very little vulnerabilities that could be exploited. The app itself, while out of scope, also had no CVE's.

4. Conclusion and Advice

4.1 Conclusion

Nothing of critical importance could be found. There was very little there in the first place, there is very few functions that could be exploited. The app couldn't be tested since it was out of scope, and there was no way for me to physically test the Bluetooth connection, which is arguably the most interesting thing of the watch.