nsbogam Update README.md History

1 contributor

39 lines (24 sloc) | 1.32 KB

ebike-jammer

Joy Ebike Wolf 2022 variant crash and deny key fob lock request

This is a report about a cyber security issue identified in Joy ebike wolf

Summary: Joy ebike Wolf variant manufactured in 2022 has a feature to lock or unlock/drive the vehicle via ebike key fob. In this vehicle, if the unlock/drive command is sniffed by Hackrf and replayed, vehicle will get unlock but it will deny lock request

Affected Product: Joy ebike Wolf, Manufacturing year 2022

Addition details URL: https://www.joyebike.com/product/wolf-bike/

Detailed report

Required Setup:

Joy ebike Wolf, Manufacturing year 2022 Joy ebike vehicle keys. Hackrf with antenna

Following steps shall be followed to achieve the Proof of concept:

1. Activate Hackrf in rx mode on 433.92 MHz
2. Press unlock/drive button on key fob
3. Hackrf captures the unlock frame command.

4. Lock the vehicle with a key.
5. Now replay the command which is captured.
6. Vehicle gets unlocked and is able to drive.
7. Press lock button on key fob
8. Vehicle deny lock button pressed from key fob and stay in unlock state.

Additional Note: Further analysis is not conducted, but multiple commands can be replayed.

Video proof of concept:

https://drive.google.com/file/d/1XDDXC2q8ZZYeujjrw4f0mW2jMsYtSGLF/view?usp=sharing

Credits : Nikhil Bogam, Krutarth Raut and Neelam Verma