nsbogam / ebike Public

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

nsbogam Update README.md ... on Jun 17 8

View code

README.md

# Joy Ebike Wolf 2022 variant replay attack to unlock the scooter

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

**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, it is possible to unlock/drive the vehicle.

**Affected Product**: Joy ebike Wolf, Manufacturing year 2022

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

**Detailed report**

**Required Setup**:

1. Joy ebike Wolf, Manufacturing year 2022
2. Joy ebike vehicle keys.
3. 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.

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

**Video proof of concept**:

https://drive.google.com/file/d/1COrBDuncLs5yR5lotpxyMSWQDY6Br-qj/view?usp=sharing

**Credits: Neelam Verma, Krutarth Raut, Nikhil Bogam**

## Releases

No releases published

## Packages

No packages published