

Tiger-Team-1337

Friday, May 13, 2022

MCK-Lock predictable rolling codes design flaw (CVE-2022-30111)

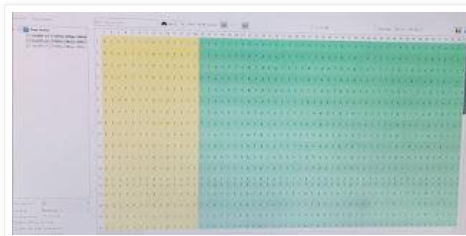
The keyspace of rolling codes for MCK Lock is predictable. It is vulnerable to replay attacks.

The methods to test:

- 1) Capture the unlock code with HackRF from the genuine MCK remote keyfob.



- 2) Replay the captured code, it will unlock the lock within 10 - 20 times attempts.



The POC Demo:

<https://www.youtube.com/watch?v=EruaGuE-cWI>

Rolling codes Hacking on RF...



at [May 13, 2022](#)

No comments:

Blog Archive

[May 2022](#) (1)
[January 2022](#) (1)
[January 2021](#) (1)
[October 2020](#) (2)

Report Abuse

Post a Comment

To leave a comment, click the button below to sign in with Google.

SIGN IN WITH GOOGLE



[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)