



# FLIPPER-ZERO ...

Is Cool Hacking Gadget ?



## About this talk ....!

- Whatever i am sharing information is completely from my experience of using flipper zero.
- not decided statements by someone else tweets or comments

And Special thanks to Prashant KV sir...!

Rockstar of  
Past null  
bangalore days



FlipperZero is really flipping the world ?



# About this device ....!

1. Flipper Zero — a Swiss Army knife for exploring access control systems..
2. Very easy to use it's just like some clicks - Plug n play type - click and play
3. Good Hardware design
4. Recovery from secondary flash
5. Open Source framework support
6. Multiple Github Repo's support

# What i liked about this device

- Not required to use so many devices to test targets
- Easy to flash frameworks
- GPIO pins for external peripherals to connect
- Device Recovery
- Looks Fancy
- CTF places it will help
- Easy to carry






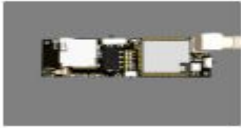








## What i don't like it ..

- You can't improve technical skill set
- Automation tool to test targets
- Left us as script kiddie

# FlipperZero Supporting devboards from different vendors

Displaying 1-36 of 61 products

Sort By:

 <p>Flipper Zero - IR Blaster Rabbitt-Labs \$27.99</p>	 <p>MAYHEM Multiboard v1.4 for Flipper Zero Cyber Bros \$55.00</p>	 <p>Flipper Zero mini esp32/nrf24/sd multi-board Cyber Bros \$89.99</p>	 <p>Flipper zero Marauder esp32, cc1101, nrf2401 rev5lab \$100.00</p>
 <p>Flipper Zero - CC1101 Expansion Board by TehRabbitt Rabbitt-Labs \$18.50</p>	 <p>Flipper Zero - Wifi Backpack - ESP32 [Kit] Binary-B \$45.00</p>	 <p>Flipper Zero WiFi Dev Board Enclosure justcallmekoko \$8.00</p>	 <p>External CC1101 MINI GPIO Board for Flipper Zero Koral \$31.99</p>
 <p>End Game Flipper Zero Wifi GPIO Module ruchus // section80 \$94.00</p>	 <p>Rabbit-labs ESP8266 board for the Flipper Zero SomeToms P2 boards \$40.00</p>	 <p>CC1101 900Mhz Module for Flipper Zero Cyber Bros \$23.99</p>	 <p>Flipper Zero - 5v NRF24 MiniBoard by TehRabbitt Rabbitt-Labs \$40.50 <del>\$45.00</del> <span>SALE</span></p>



# Flipper-zero can't save his a.. From crash bugs?



<https://vvx7.io/posts/2022/09/your-amiibos-haunted/>



# CVE

## CVE-2022-40363 Detail

### Description

A buffer overflow in the component nfc\_device\_load\_mifare\_ul\_data of Flipper Devices Inc., Flipper Zero before v0.65.2 allows attackers to cause a Denial of Service (DoS) via a crafted NFC file.

### Severity

CVSS Version 3.x

CVSS Version 2.0

#### CVSS 3.x Severity and Metrics:



NIST: NVD

Base Score: 5.5 MEDIUM

Vector:

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H



Time for  
Q&A