TEARDOWN OF AN EV CHARGER FOR SECURITY RESEARCH

AND WHEN EV CHARGERS ATTACK!

AGENDA

Whoami

Introduction

Known Exploits

Teardown

Demo

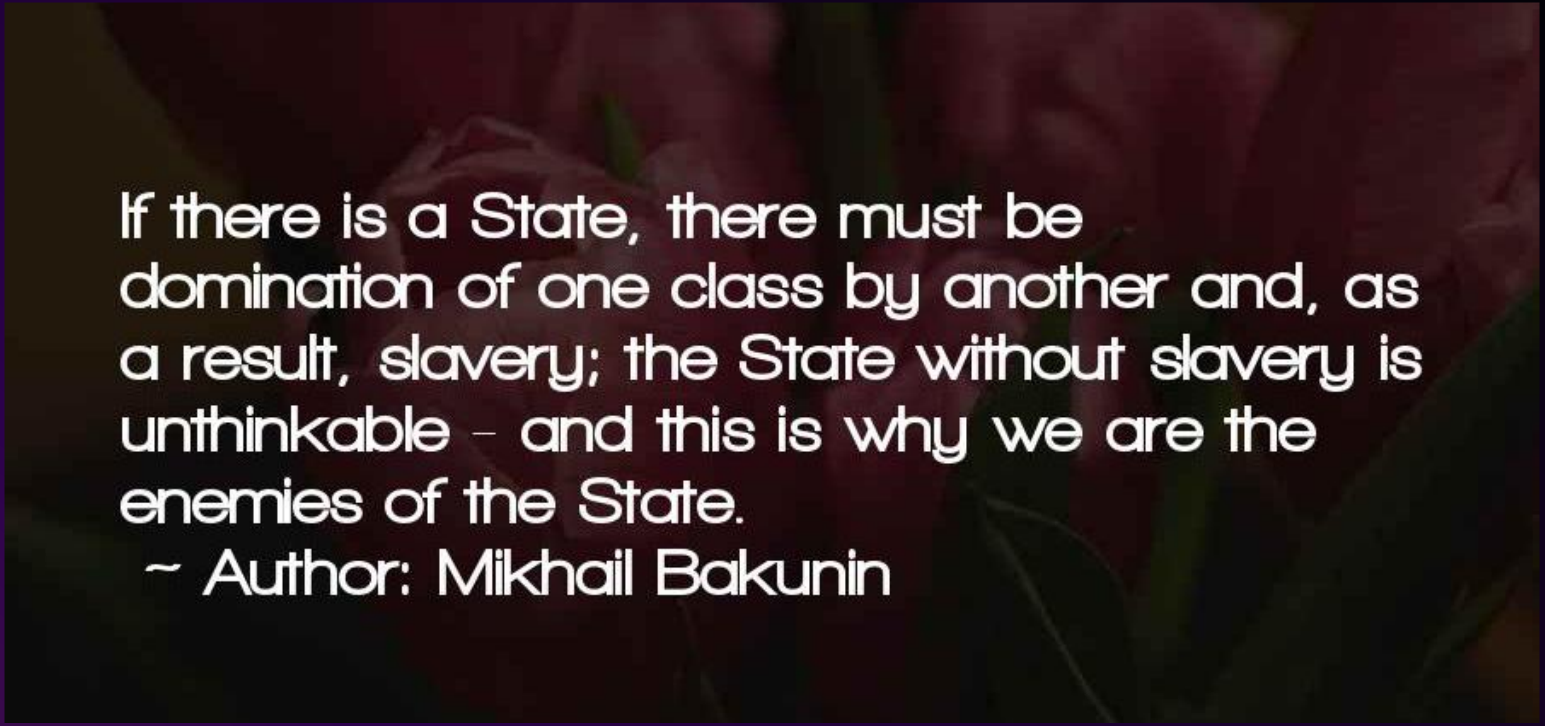
WHOAMI

- Jay Turla
- Principal Security Researcher at VicOne
- Car Hacking Village Philippines (village chief)
  > https://www.facebook.com/chvdotph
- ROOTCON Goon (organizer)
- SpiritCyber-24 Finalists
- Hack-A-Sat 2020 Finalists

INTRODUCTION

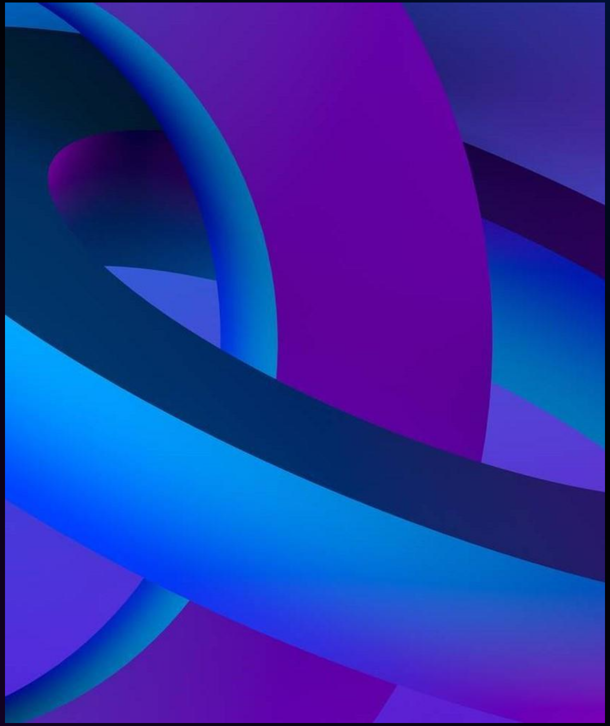
EV CHARGERS?

WHAT STATE ARE WE?

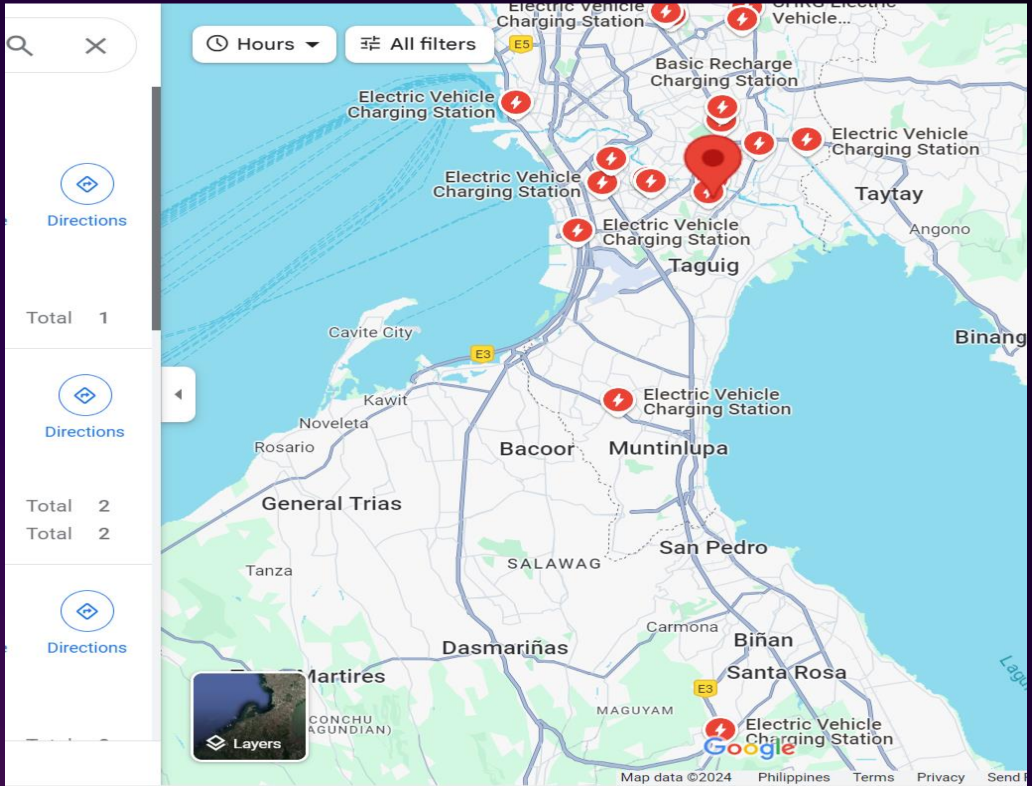


If there is a State, there must be domination of one class by another and, as a result, slavery; the State without slavery is unthinkable - and this is why we are the enemies of the State.

~ Author: Mikhail Bakunin



EV CHARGING STATIONS IN LUZON AND CEBU


Directions

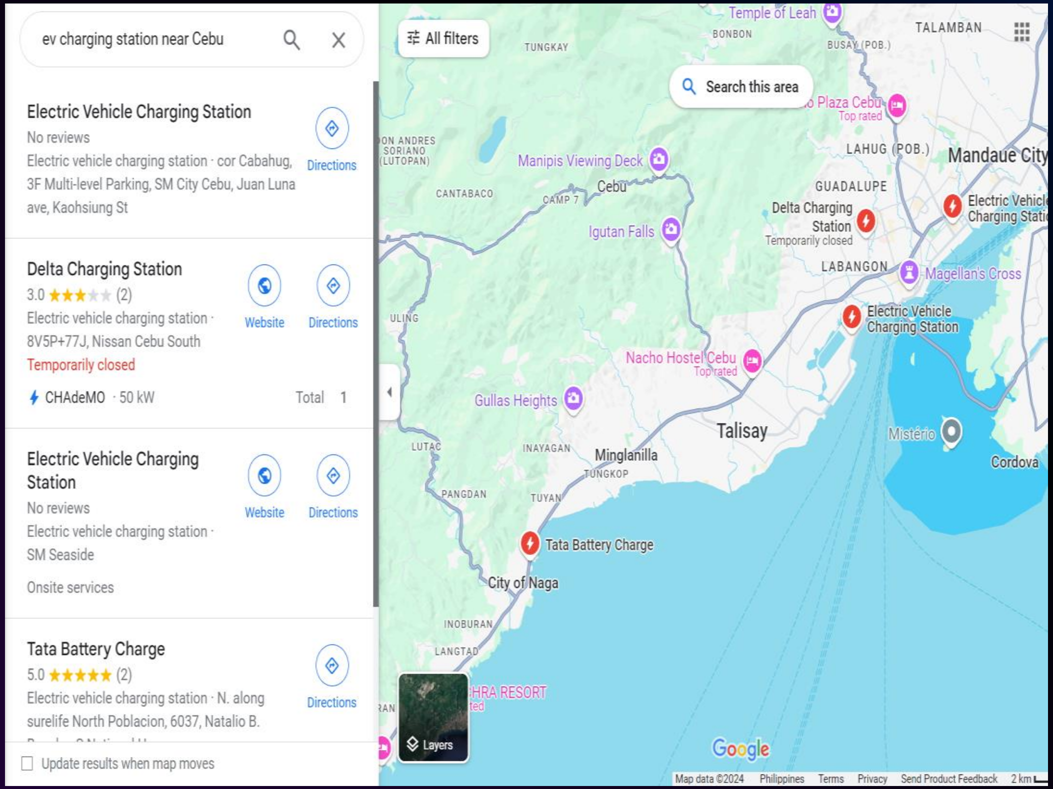
Total 1

Directions

Total 2
Total 2

Directions

Hours
All filters
Electric Vehicle Charging Station
Vehicle...
Basic Recharge Charging Station
Electric Vehicle Charging Station
Electric Vehicle Charging Station
Electric Vehicle Charging Station
Electric Vehicle Charging Station
Taytay
Angono
Taguig
Cavite City
Binang
E5
E3
Kawit
Noveleta
Rosario
Electric Vehicle Charging Station
Bacoor
Muntinlupa
General Trias
San Pedro
Tanza
SALAWAG
Carmona
Dasmariñas
Biñan
Santa Rosa
Martires
CONCHU AGUNDIAN)
MAGUYAM
E3
Electric Vehicle Charging Station
Layers
Google
Map data ©2024
Philippines
Terms
Privacy
Send


ev charging station near Cebu

Electric Vehicle Charging Station
No reviews
Electric vehicle charging station · cor Cabahug, 3F Multi-level Parking, SM City Cebu, Juan Luna ave, Kaohsiung St
Directions

Delta Charging Station
3.0 ★★★★★ (2)
Electric vehicle charging station · 8V5P+77J, Nissan Cebu South
Temporarily closed
CHAdeMO · 50 kW
Total 1
Website
Directions

Electric Vehicle Charging Station
No reviews
Electric vehicle charging station · SM Seaside
Onsite services
Website
Directions

Tata Battery Charge
5.0 ★★★★★ (2)
Electric vehicle charging station · N. along surelife North Poblacion, 6037, Natalio B.
Directions

□ Update results when map moves

EV CHARGING STATIONS IN PH

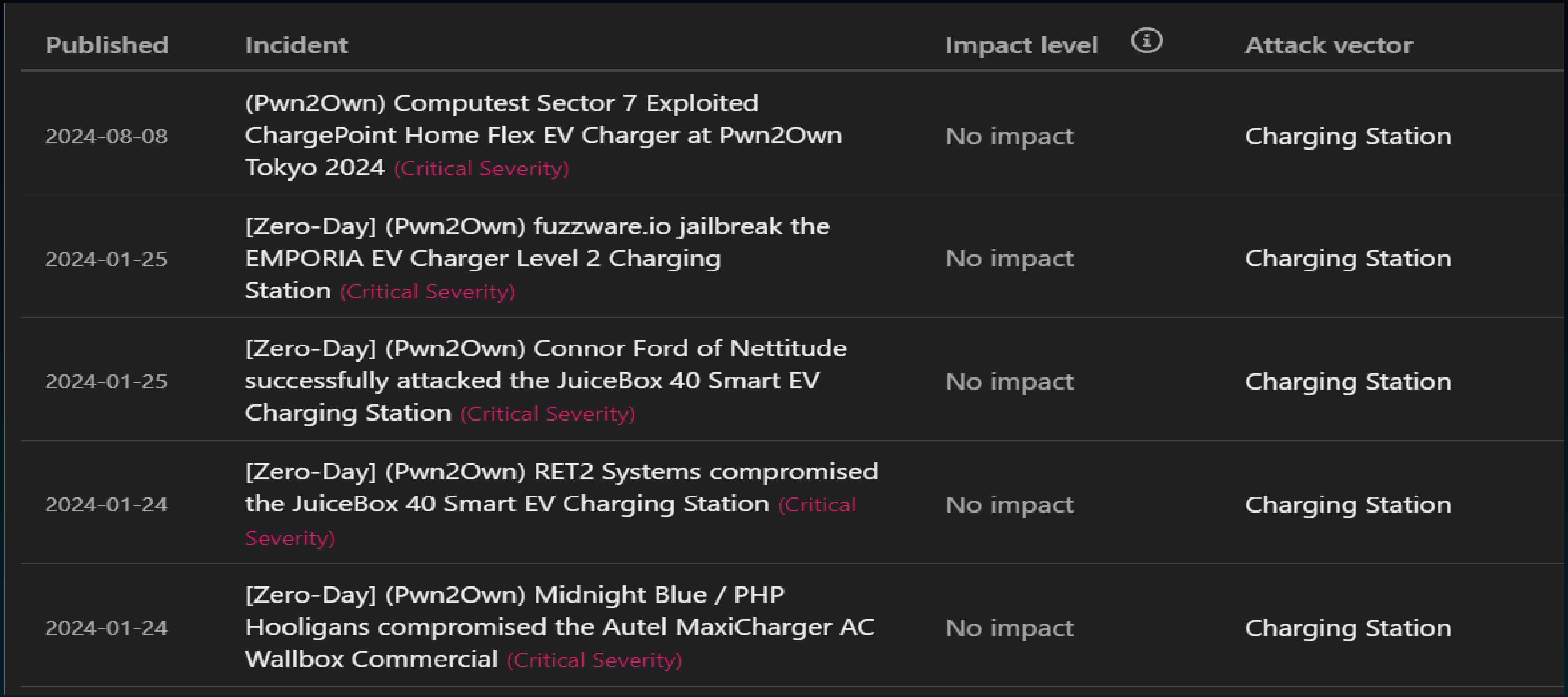
EV charging stations are starting to rise…

We see them in the malls… (free)

We see some distributors have pay to charge

Some are not in Google maps yet…

Known Exploits from Pwn2Own Automotive 2024



Published	Incident	Impact level ⓘ	Attack vector
2024-08-08	(Pwn2Own) Computest Sector 7 Exploited ChargePoint Home Flex EV Charger at Pwn2Own Tokyo 2024 (Critical Severity)	No impact	Charging Station
2024-01-25	[Zero-Day] (Pwn2Own) fuzzware.io jailbreak the EMPORIA EV Charger Level 2 Charging Station (Critical Severity)	No impact	Charging Station
2024-01-25	[Zero-Day] (Pwn2Own) Connor Ford of Nettitude successfully attacked the JuiceBox 40 Smart EV Charging Station (Critical Severity)	No impact	Charging Station
2024-01-24	[Zero-Day] (Pwn2Own) RET2 Systems compromised the JuiceBox 40 Smart EV Charging Station (Critical Severity)	No impact	Charging Station
2024-01-24	[Zero-Day] (Pwn2Own) Midnight Blue / PHP Hooligans compromised the Autel MaxiCharger AC Wallbox Commercial (Critical Severity)	No impact	Charging Station

What to gain from exploiting it?

- Botnet system
- Free charging by bypassing the API payment gateway
- C2 server?

Quick Testing Methodology

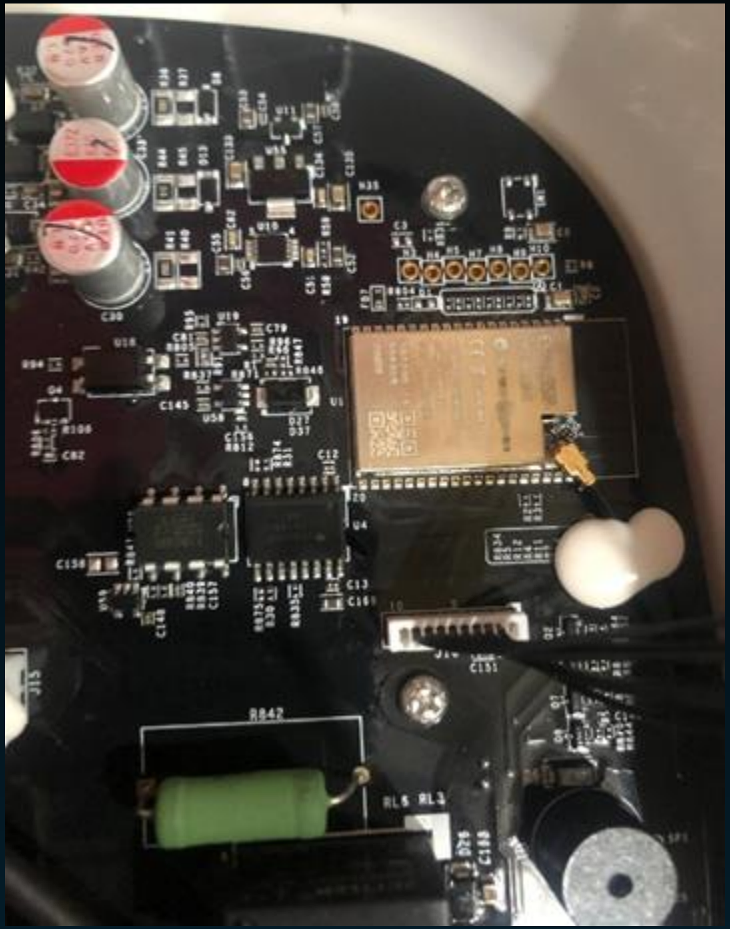
- Check for IP addresses and scan for open ports

Check for debug ports.

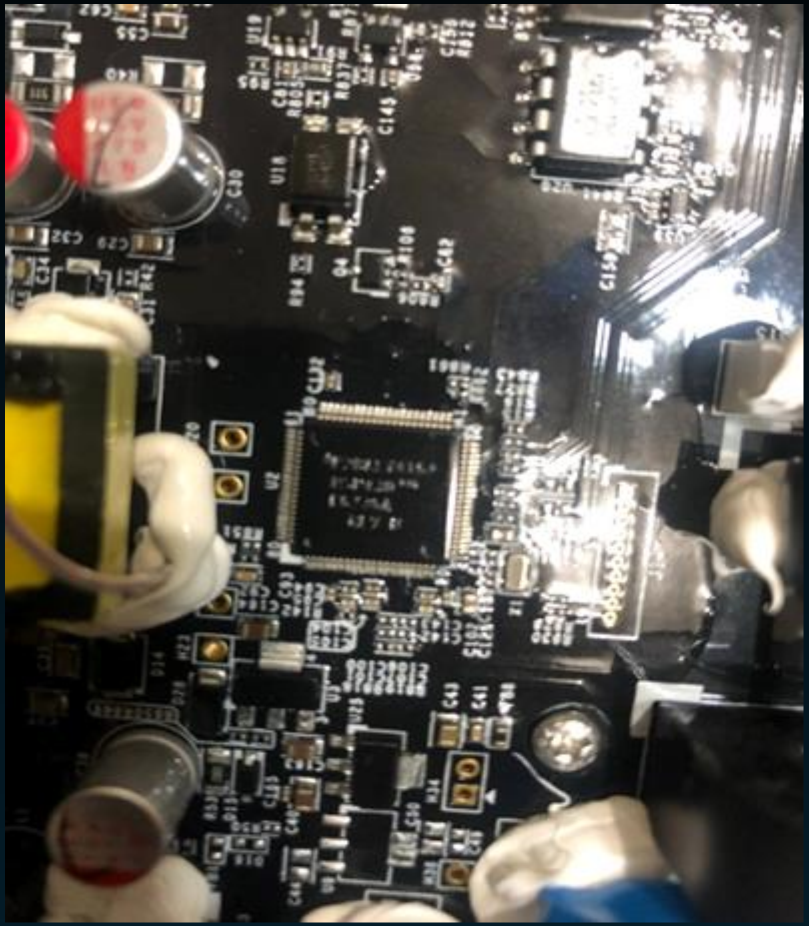
- Test mobile interfacing apps.
- Check for firmware upload / signature verification.
- Sniff firmware upgrades.
- Check for buffer overflows on its services.

DIRECTPOWER360
Future cars will have higher power batteries for faster charging
Nidec

EV Charger Teardown of Emporia

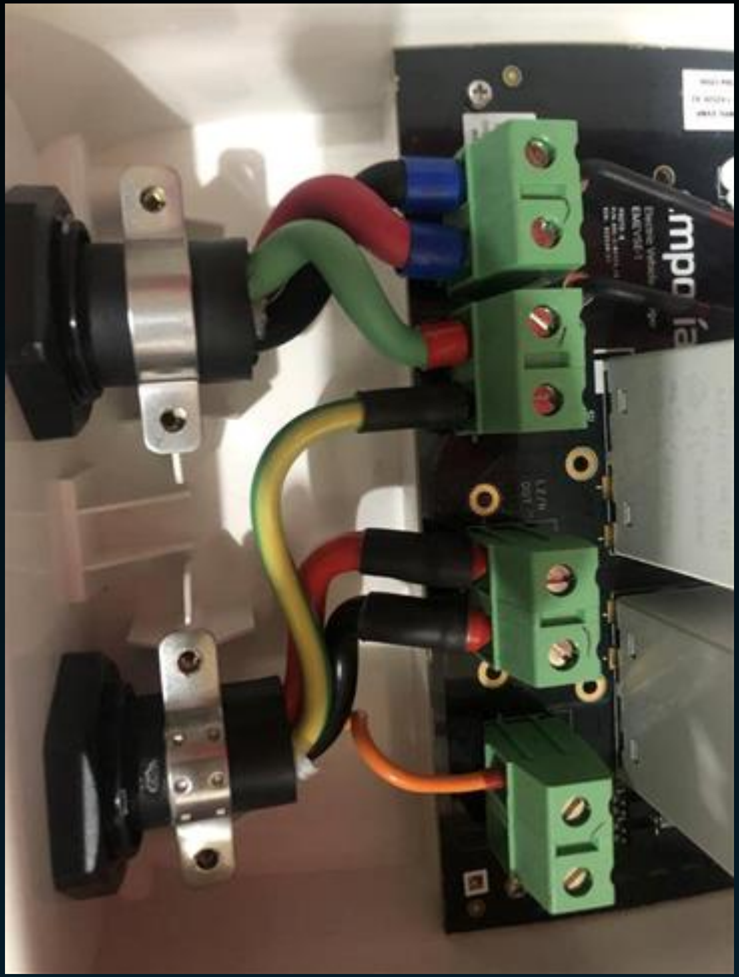


ESP32 Microcontroller with exposed serial interfaces

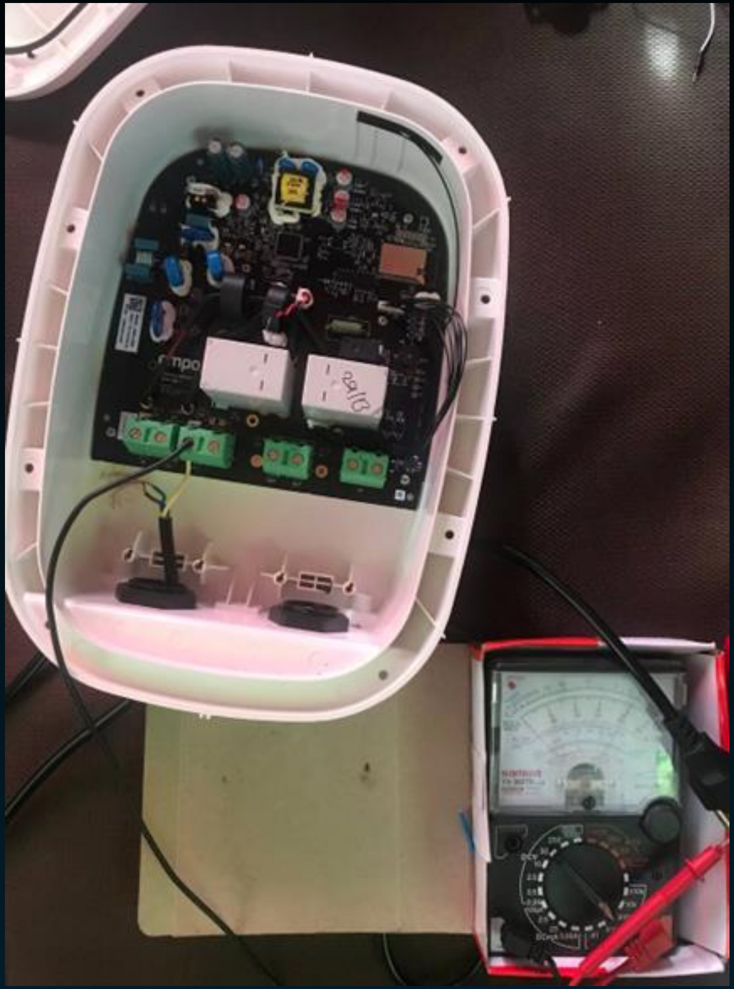


TI MSP 430 F6736A for sensors and metrology

EV Charger Teardown of Emporia



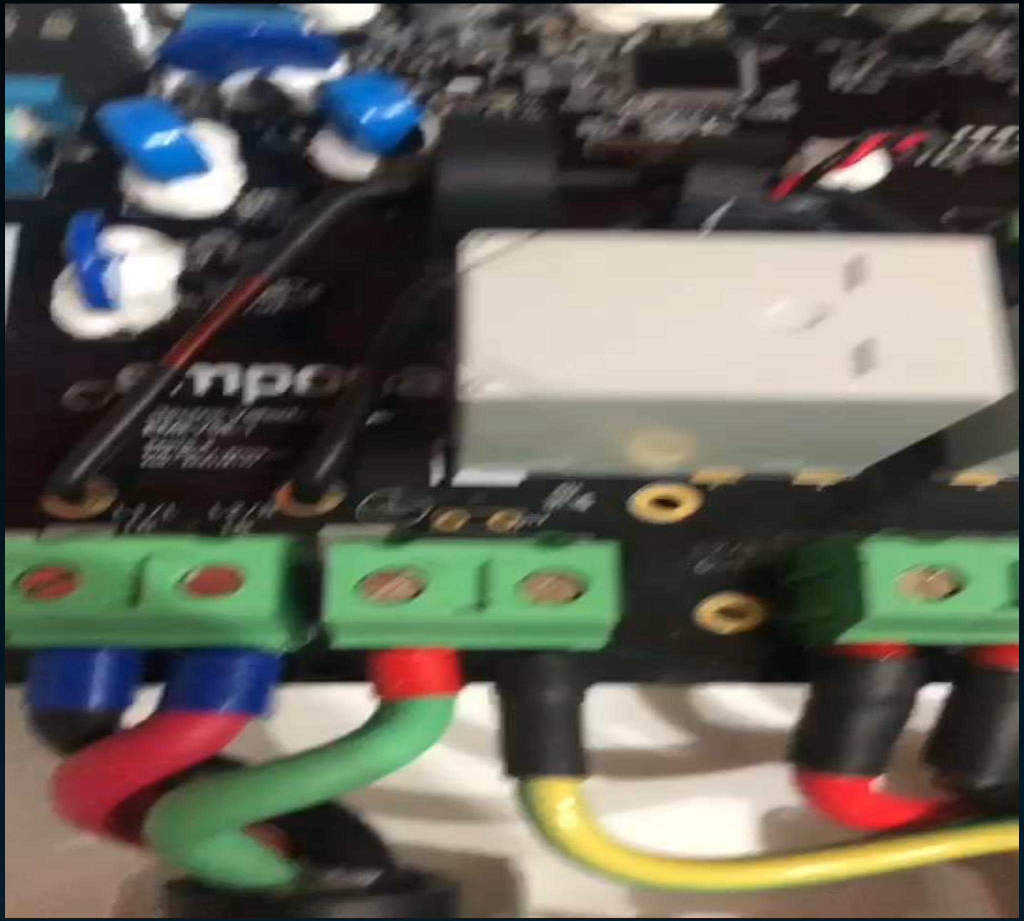
Input and Output Power connectors



Replacement of 3-pronged cables

Powering it up

Teardown preview



Emporia EV Charger Pwn2Own Survery 2024 (Easy to spot)

- Buffer overflow on WiFi
- Required handling on all WiFi channels
- Can extract firmware via esptool
- Lack of bounds checks on data
- Firmware updates are signed & verified, but in plaintext

DEMO

THANK YOU

Jay Turla

Principal Security Researcher

VicOne