# Electric Vehicle Chargers: Survey of devices from Pwn2Own Automotive 2024

Presented by Jonathan Andersson

The Zero Day Initiative & Trend Micro Research

# Presentation Acknowledgements

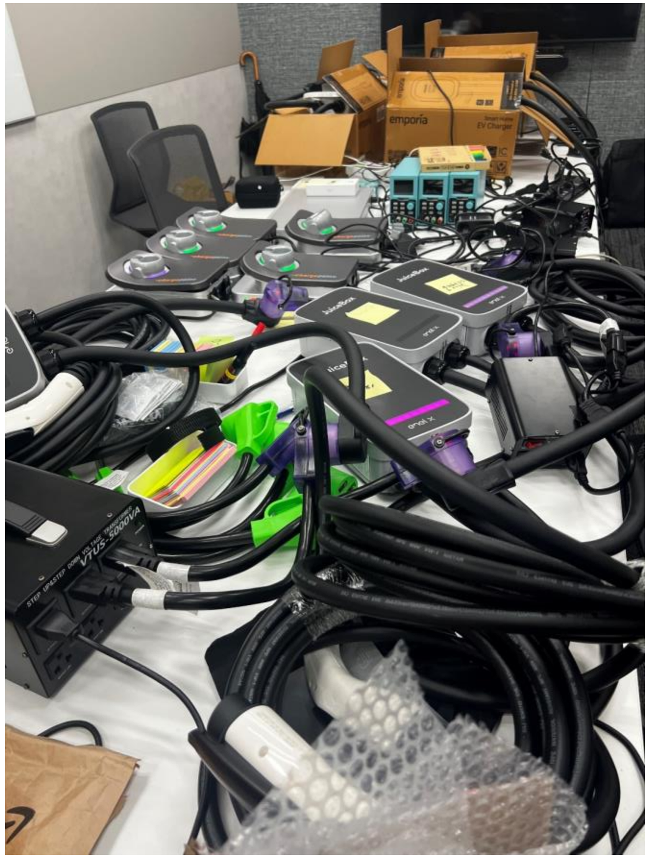
This presentation benefited from the support of VicOne, Trend Micro and the numerous security researchers that participated in Pwn2Own Automotive 2024, as well as from independent research by Trend's Advanced Security Research Team (ASR) & The Zero Day Initiative (ZDI).

# Pwn2Own Automotive 2024 @ Tokyo Big Sight

# Pwn2Own Automotive 2024 - Setup

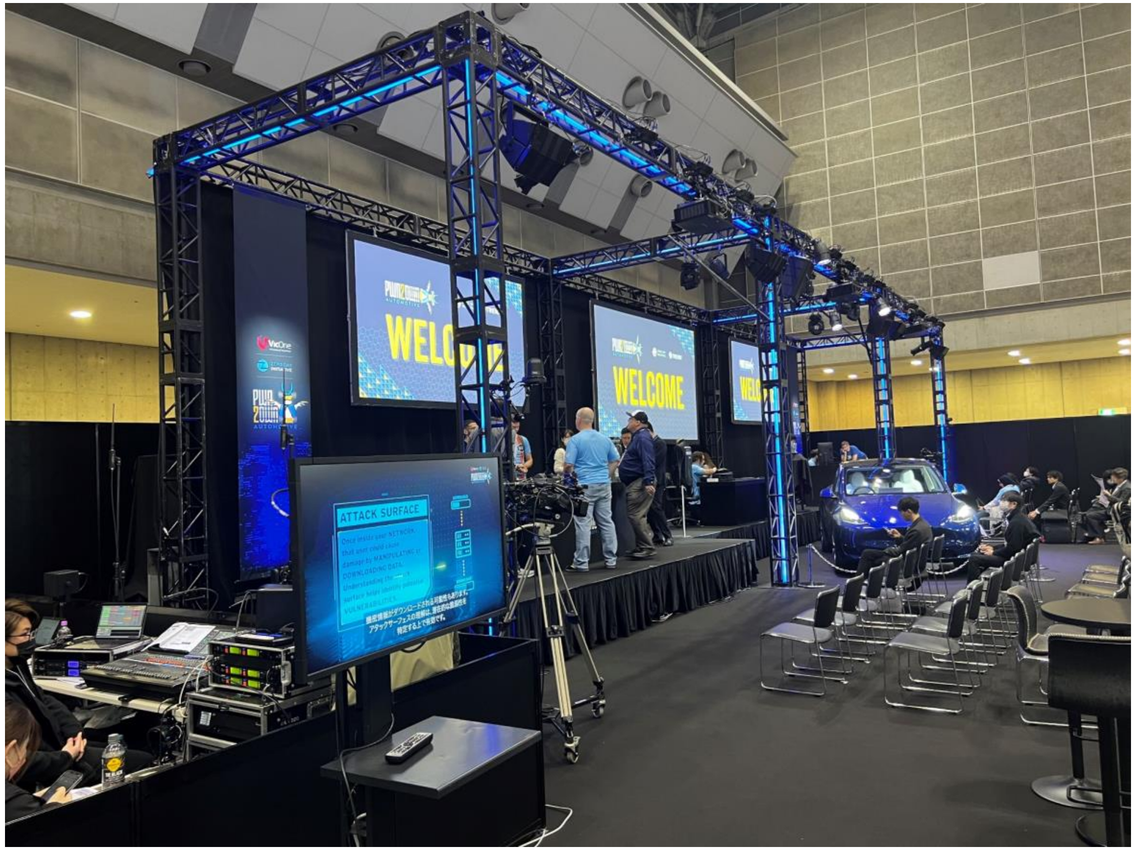
Ship 200 ft$^3$ (1/3 gray whale)

Unpack

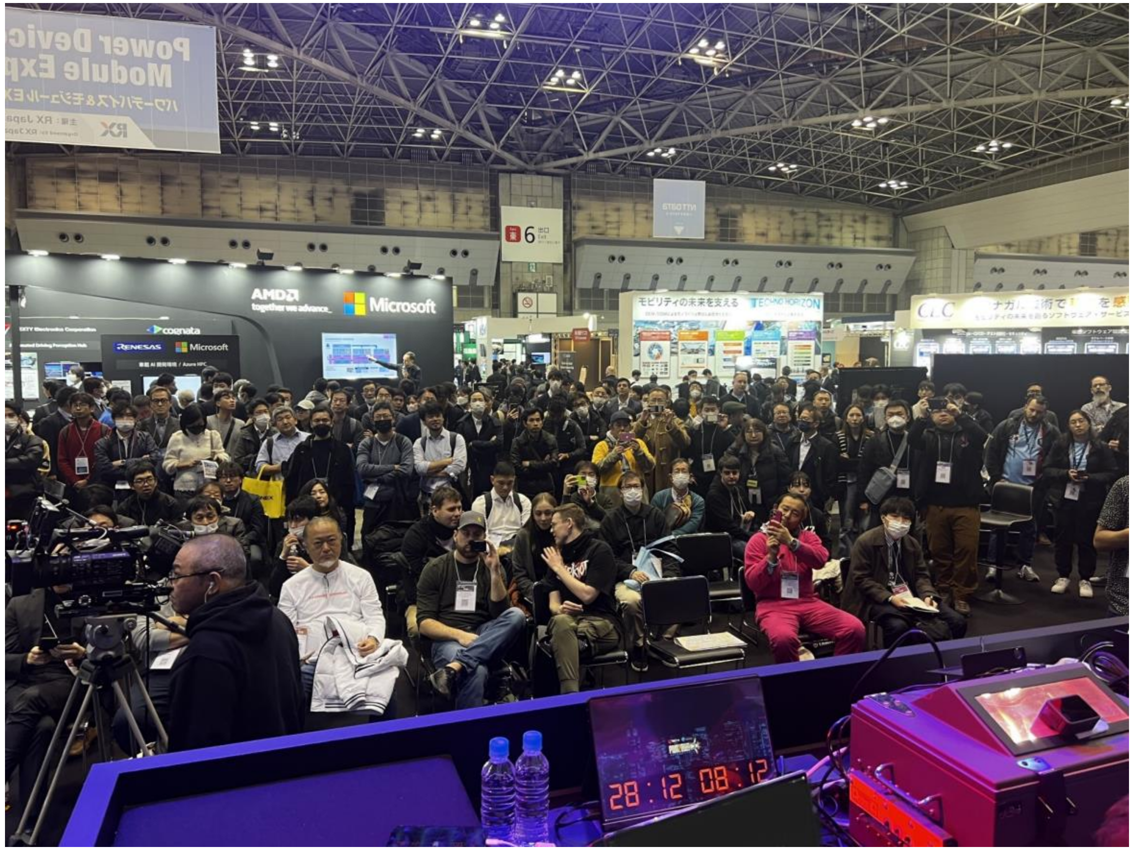


Configure

# Pwn2Own Automotive 2024 - Event

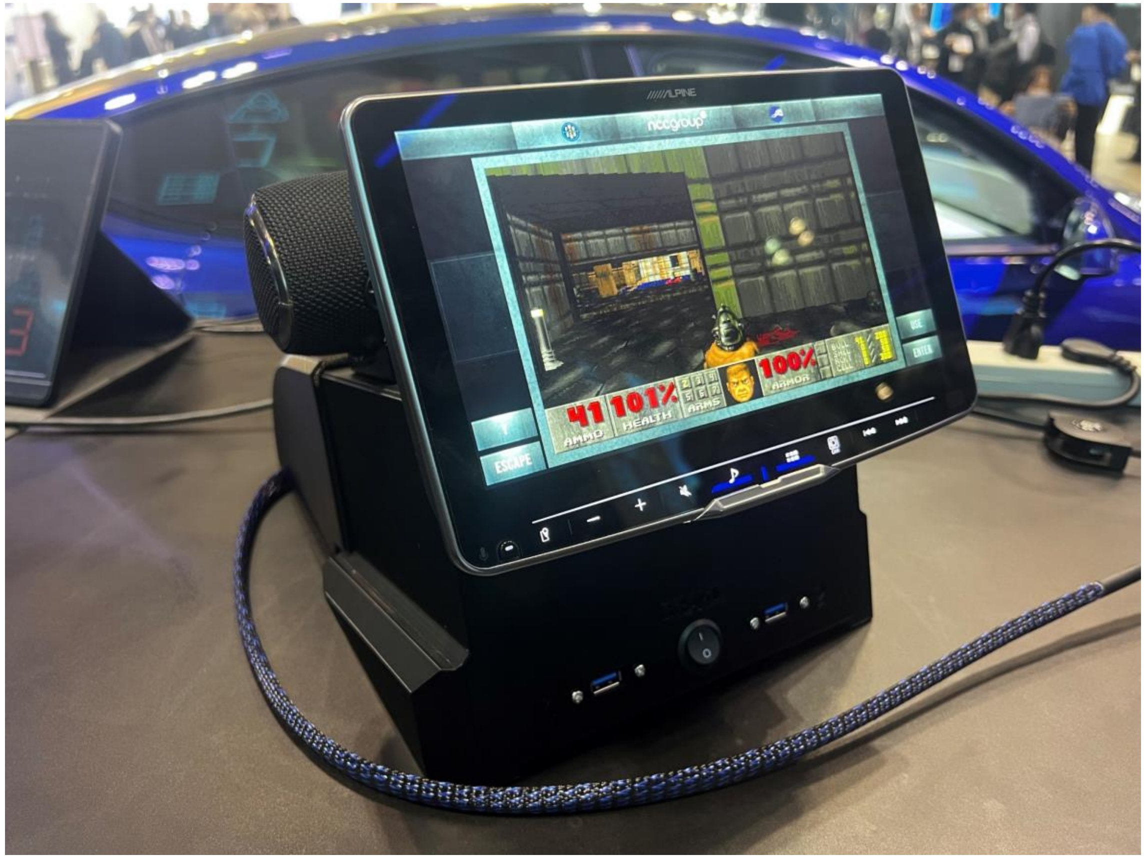


Stage

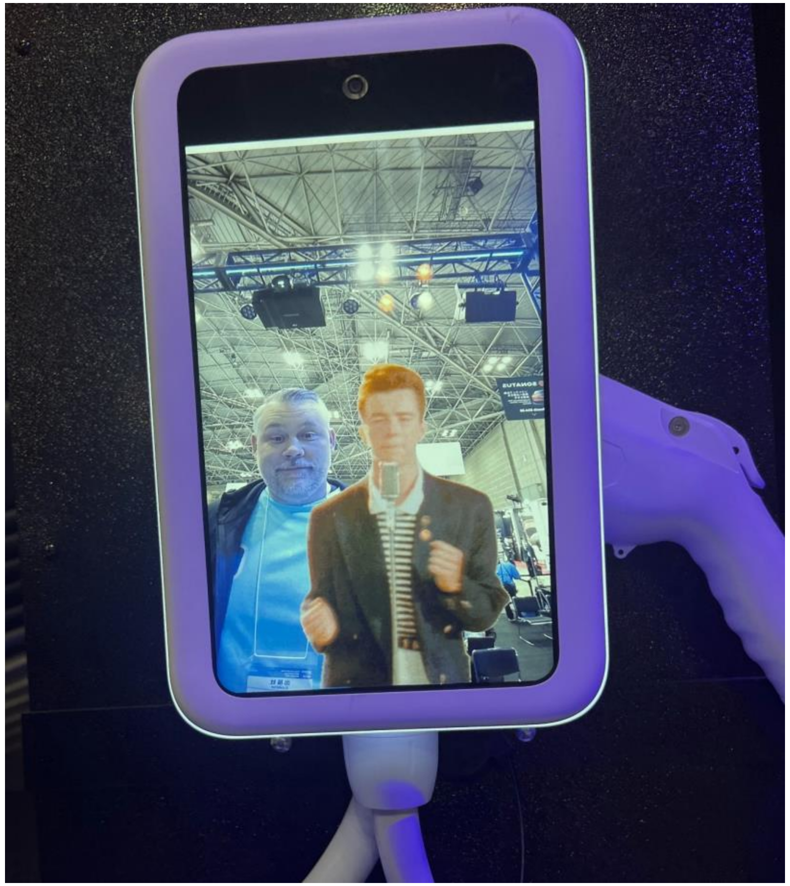


Audience @ Tesla Attempt

# Pwn2Own Automotive 2024 - Exploits



NCC Group – Playable Doom on Alpine



Sina – Live Video Rickroll on Ubiquity

# Pwn2Own Automotive 2024 - Results

- ~$1.3M USD Total
- Master of Pwn Leaderboard:
  - Synactiv $450,000
  - Fuzzware.io $177,500
  - Midnight Blue / PHP Hooligans $80,000
  - NCC Group EDG $90,000
  - Computest Sector 7 $67,500

# Pwn2Own Automotive 2024 - Vulnerabilities

| Category | Number |
|---|---|
| EV Chargers | 26 |
| In-Vehicle Infotainment (IVIs) | 14 |
| OS | 4 |
| Tesla | 5 |
| Internal Finds | 16 |
| Total | 65 |

# Pwn2Own Automotive - Electric Vehicle Charger Category

# Consumer EV Charger Designs - Hardware

- Designs typically feature at least two major subsystems
  1. Application processor subsystem (GUI / Network interfaces)
  2. Power supply, metering & control circuitry
- Key components/systems observed
  - Display Modules
  - Memories – Flash / RAM
  - Ethernet, Wi-Fi, Bluetooth, LTE
  - TPM
  - CAN
  - NFC / RFID
  - Cameras
  - SAE J1772 (Standard EV charger plug)
  - Serial console / JTAG / debug ports
  - Power Relays

# Consumer EV Charger Designs - Hardware

- Many devices had serial interfaces available
- Several devices had JTAG/debugging interfaces enabled
- Many use off the shelf SoC/SoM for application processor
  - ESP32 module variants & Silicon Labs WGM Series modules
- Operating system can vary from RTOS to Linux and Android
- Multiple firmwares are running in a typical EV charger

# Consumer EV Charger Designs - Mobile Applications

- Every charger discussed has an associated mobile application
- Communicate with the charger over Bluetooth
- Used for configuration
- Often are responsible for firmware updates
- Disassembling mobile apps provides useful information
- An easy way to get started understanding the chargers

# Consumer EV Charger Designs - Networks

- Configuration occurs over Bluetooth
- Charger connects to local network
- Some have cellular network interfaces (SIM cards accessible)
- Charger connects out to vendor cloud
- Cloud handles user authentication for charging

# Consumer EV Chargers - Attack Surfaces

- Mobile application & Bluetooth LE for configuration
- Wi-Fi & Ethernet connections
- Listening network services
  - OCPP, MQTT, HTTP/S, Telnet, SSH
- Connection to the cloud
- Firmware update process

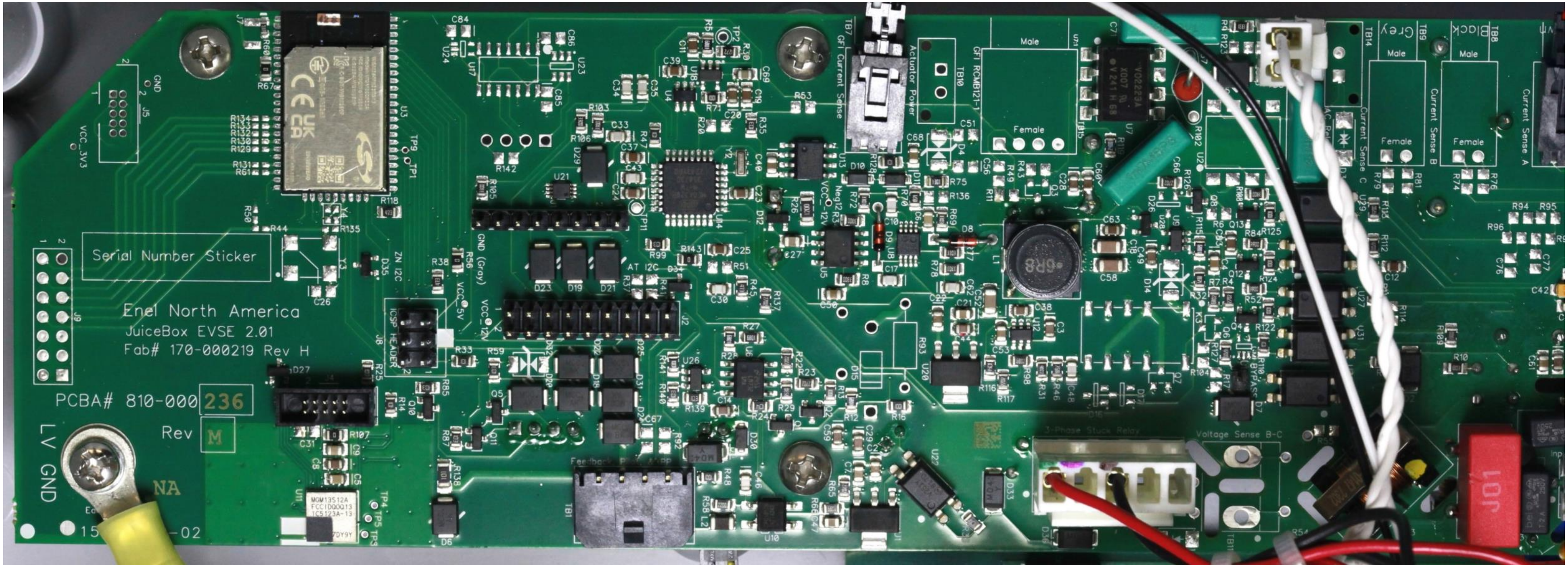
# Enel Juicebox

- Single PCB design
- Application CPU
  - Silicon Labs WGM160P22A SoM (ARM Cortex M4)
- Metrology
  - Atmel Mega 328P (AVR RISC microcontroller)
  - Atmel M90E36A energy metering chip

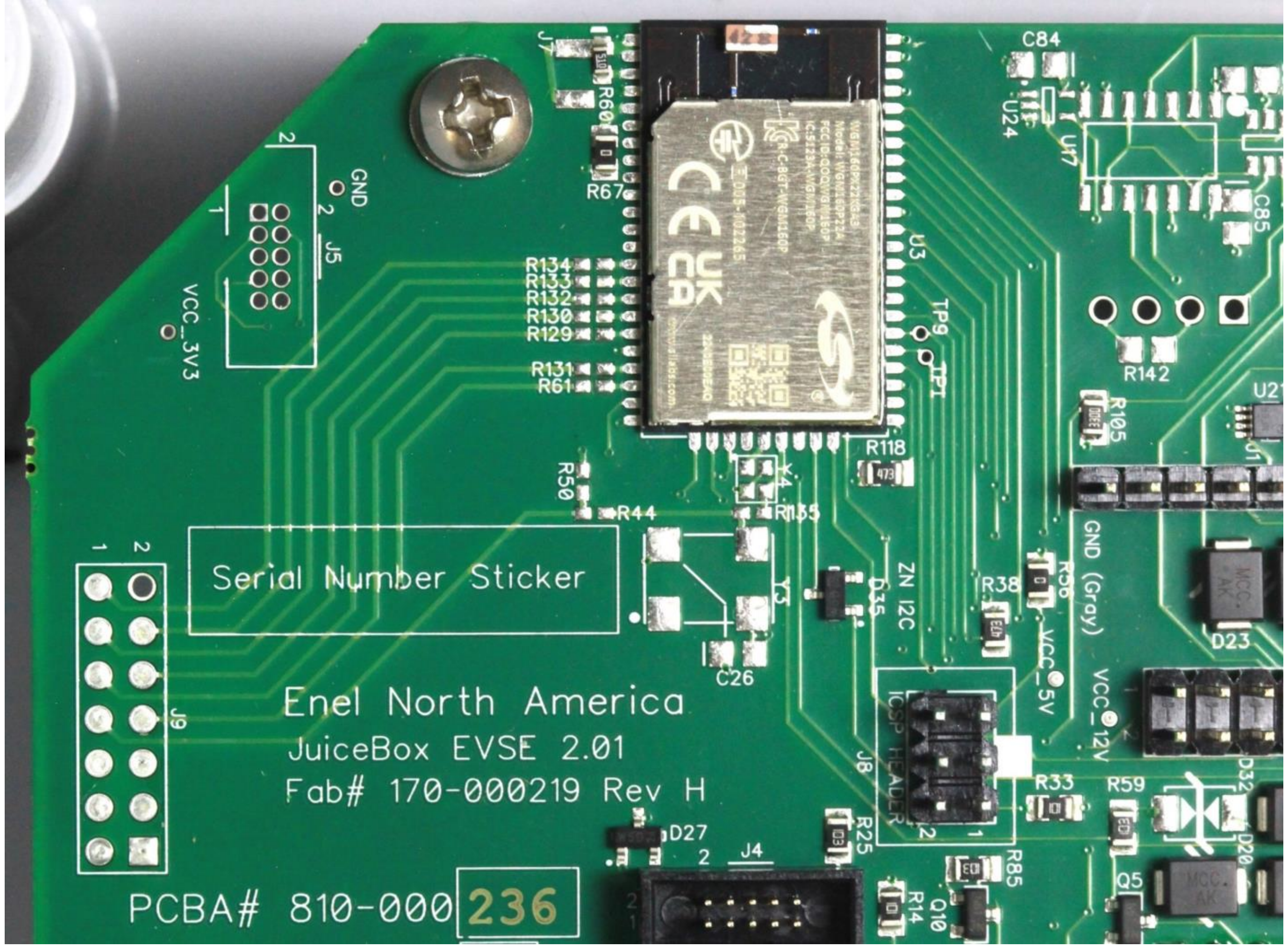
# Enel Juicebox Available Security Features

- Silicon Labs WGM160P22A SoM
  - EOL Gecko OS
  - Lacks security protections
- Atmel Mega 328P
  - Not recommended for new designs
  - Boot loader can be locked
- Atmel M90E36A
  - No security features

# Enel Juicebox PCB



# Enel Juicebox Silicon Labs WGM160P22A SoC



# Enel Juicebox Silicon Labs WGM160P22A SoC

- Silicon Labs includes a telnet port in the Gecko OS
- The Gecko OS management interface is listening on Wi-Fi
- This service exports a suite of powerful commands
  - https://docs.silabs.com/gecko-os/4/standard/4.2/cmd/commands

# Enel Juicebox in Pwn2Own Automotive 2024

- Number of attempts: 6 total
  - 3 Full Win
  - 1 Success/Collision
  - Remote management features made it a relatively easy target
  - Exploits involved shell code injection by stack buffer overflow

# Enel Juicebox Security Conclusions

- Use of Silicon Labs Gecko OS
  - End-of-life Gecko OS
  - Exposes powerful network service that allows configuration of the device, including enabling other vulnerable services
- Lack of mitigations
  - No stack cookies
  - No memory protections (executable stack & heap)

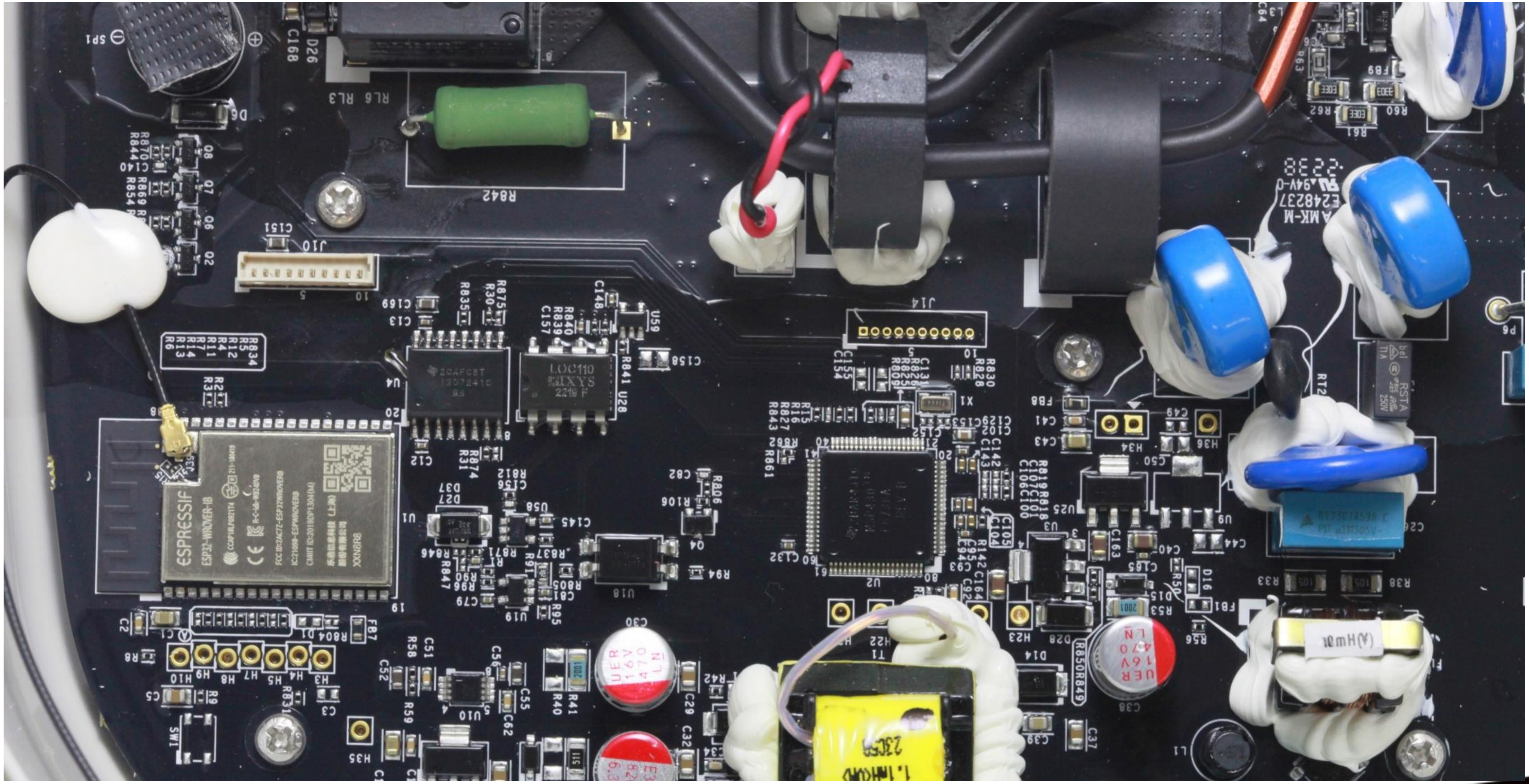
# Emporia Smart Home EV Charger

- Single PCB design
- Application CPU
  - ESP32-WROOM-1B (Xtensa)
  - Exposed serial programming port
- Metrology
  - TI MSP 430 F6736A

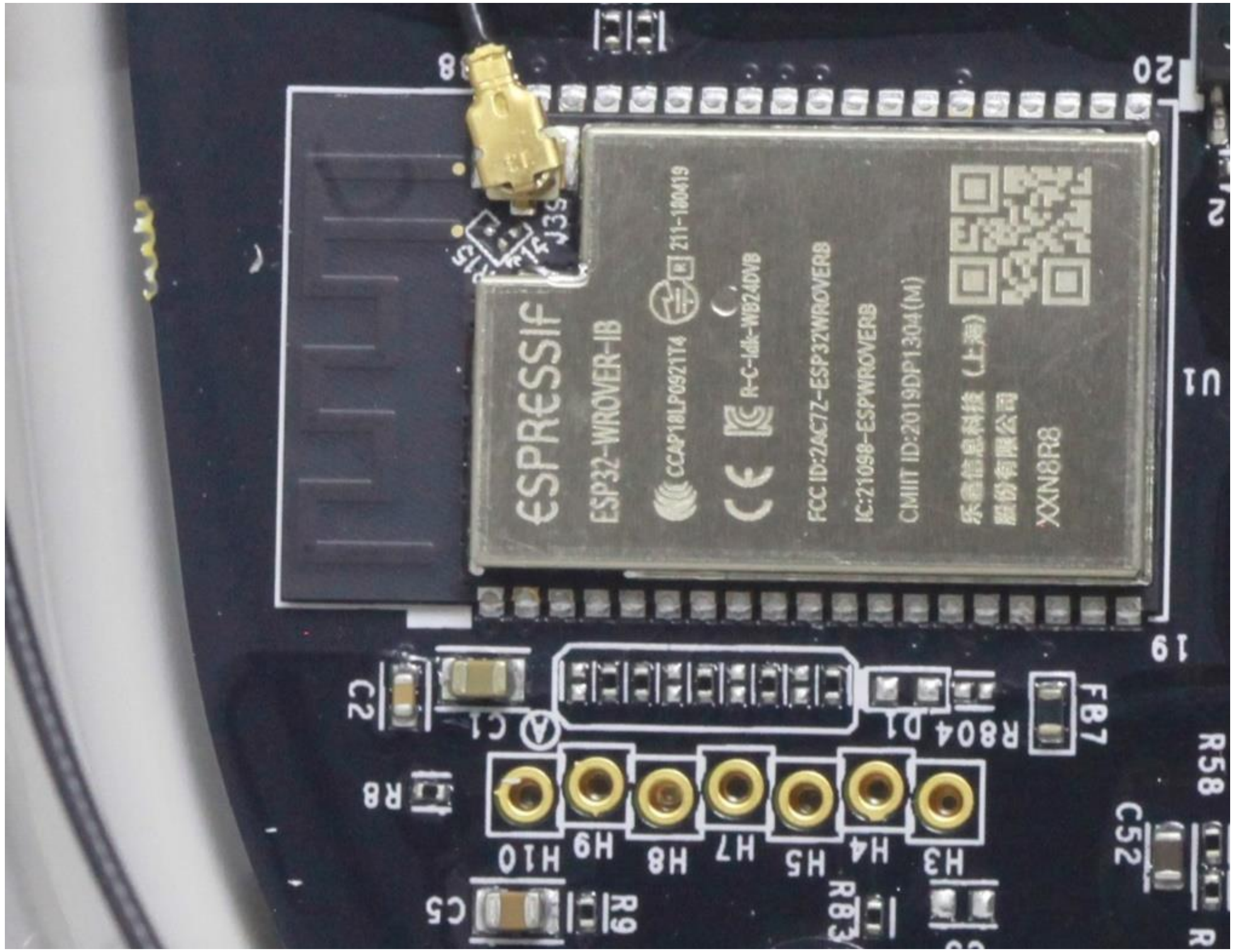
# Emporia Smart Home EV Charger Available Security Features

- Application CPU
  - ESP32-WROOM-1B (Xtensa)
  - Provides OTP to configure security features
  - JTAG can be permanently disabled
  - Supports encryption of RAM and flash
  - Supports glitching detection
- Metrology
  - TI MSP 430 F6736A
  - eFuse (soft)
  - JTAG/Spy-By-Wire (SBW) debugging locks
  - JTAG can be permanently locked by locking bootstrap loader

# Emporia Smart Home EV Charger PCB



# Emporia Smart Home EV Charger ESP32 – Serial Interface



- Can extract firmware
- H5 - Serial RX
- H7 - Serial TX
- H8 - Ground
- H10 - GPIO 0
  - Pull to ground to enable ESP32 tools

# Emporia Smart Home EV Charger in Pwn2Own Automotive 2024

- Number of attempts: 2 total
  - 1 Full Win
  - Vulnerability affecting Wi-Fi
  - Resulting in a buffer overflow
  - Required handling all Wi-Fi channels

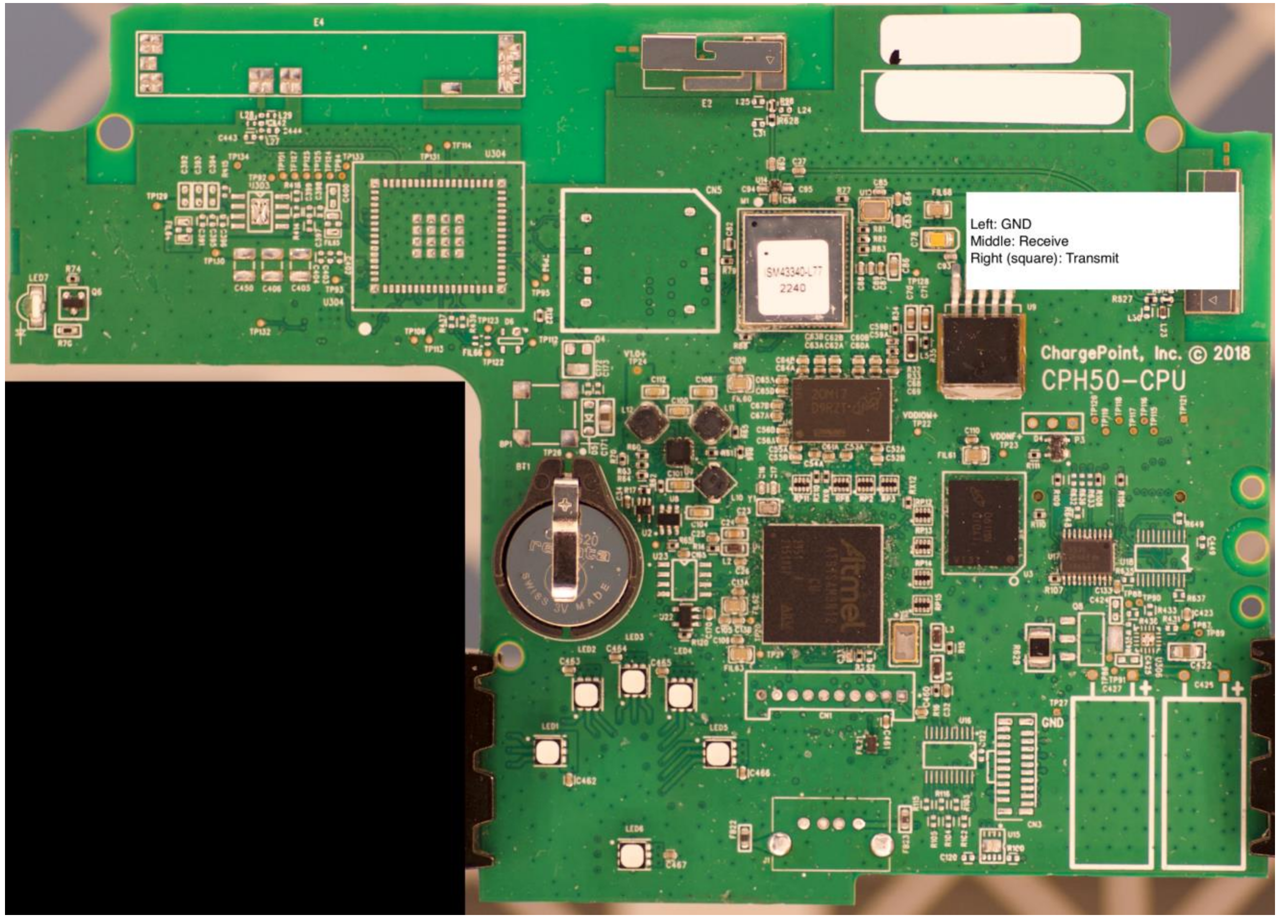
# Emporia Smart Home EV Charger Security Conclusions

- Lack of bounds checks on data
- Lack of ASLR aided exploitation
- Use of global variables aided exploitation
- Mishandling of unauthenticated data
- Firmware updates are signed & verified, but in plaintext

# ChargePoint Home Flex Architecture

- Dual-PCB Design
- CPU Board
  - ATMEL AT91SAM9N12 (ARM9)
  - Linux OS
  - Bluetooth
  - Wi-Fi
- Metrology Board
  - TI MSP430 F6765

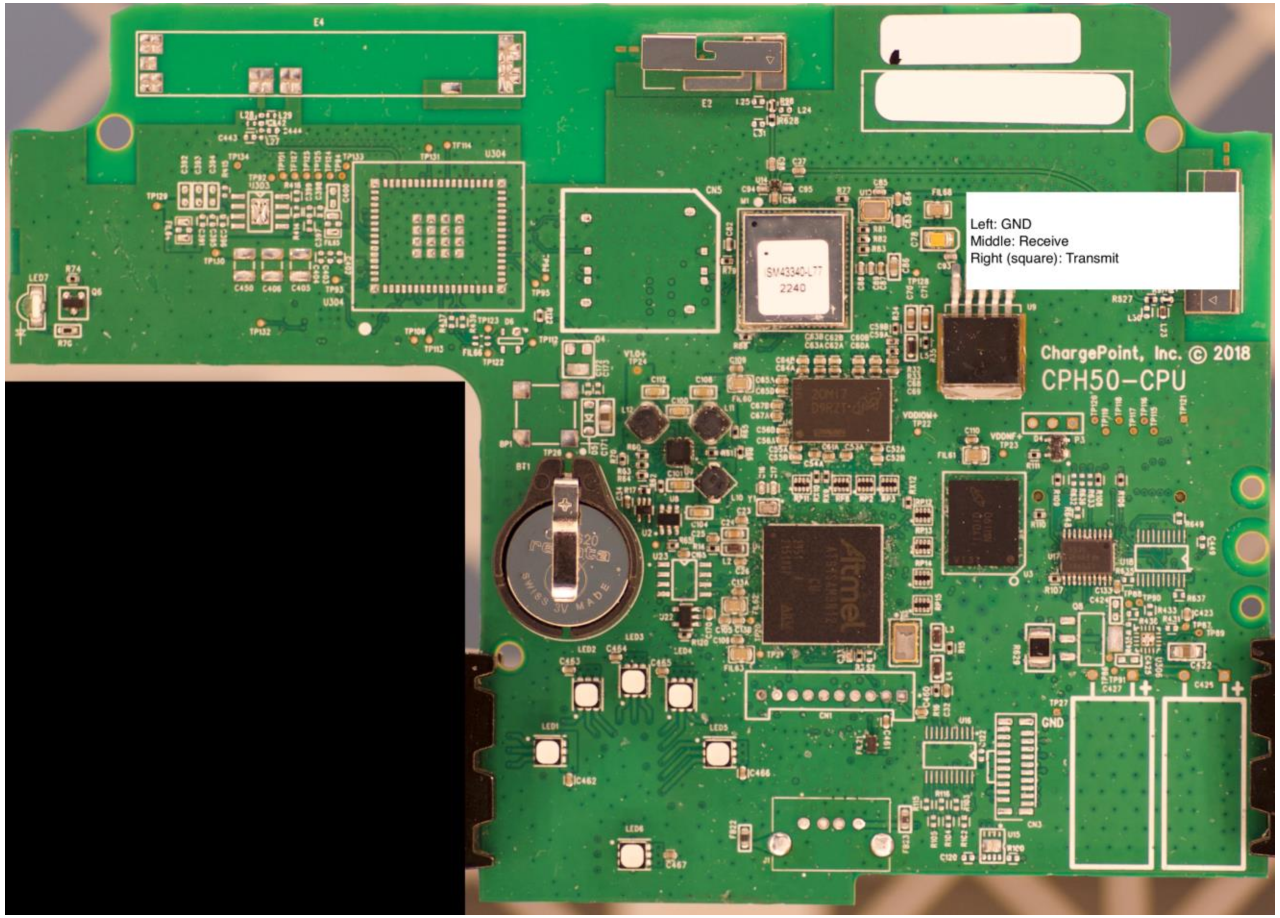
# ChargePoint Home Flex CPU Board



Left: GND
Middle: Receive
Right (square): Transmit

- Atmel AT91SAM9N12
- External flash storage
- Exposed serial
- Exposed JTAG
- Wi-Fi
- Bluetooth
- USB

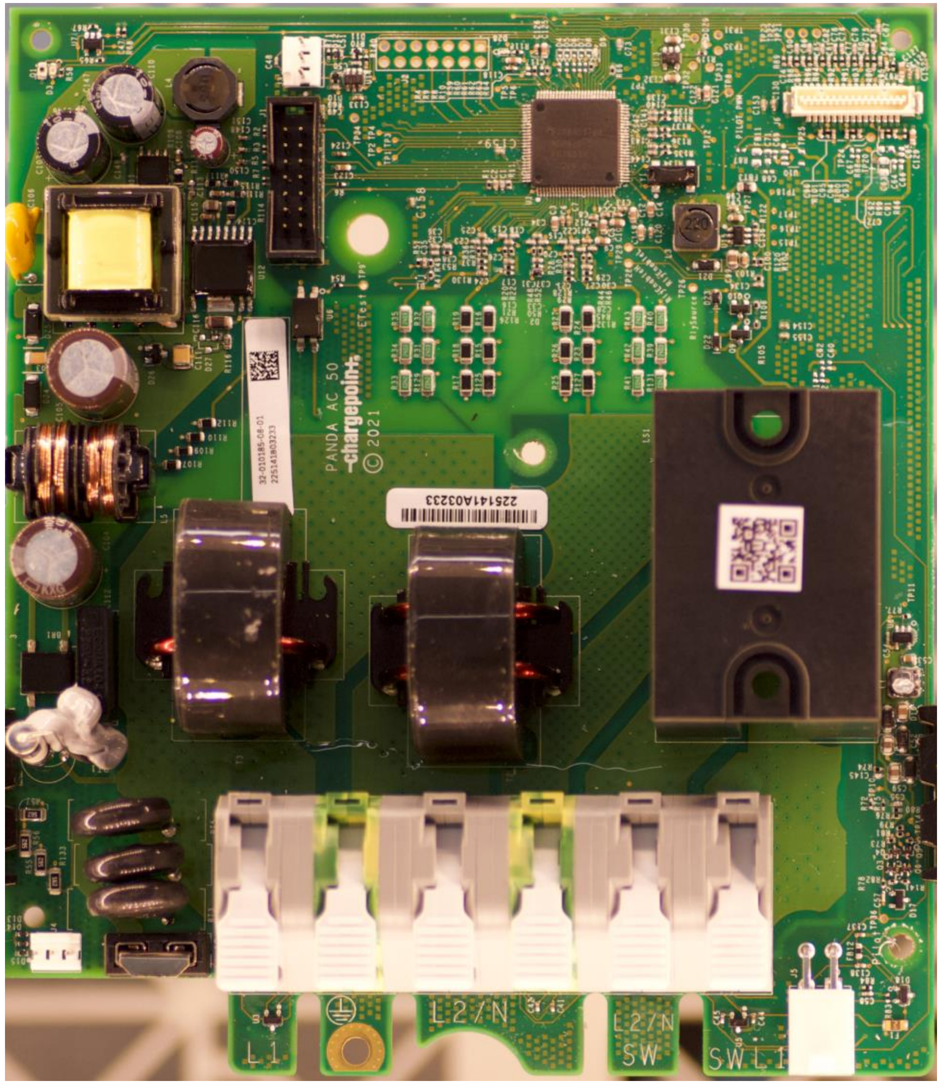
# ChargePoint Home Flex CPU Board Available Security Features



Left: GND
Middle: Receive
Right (square): Transmit

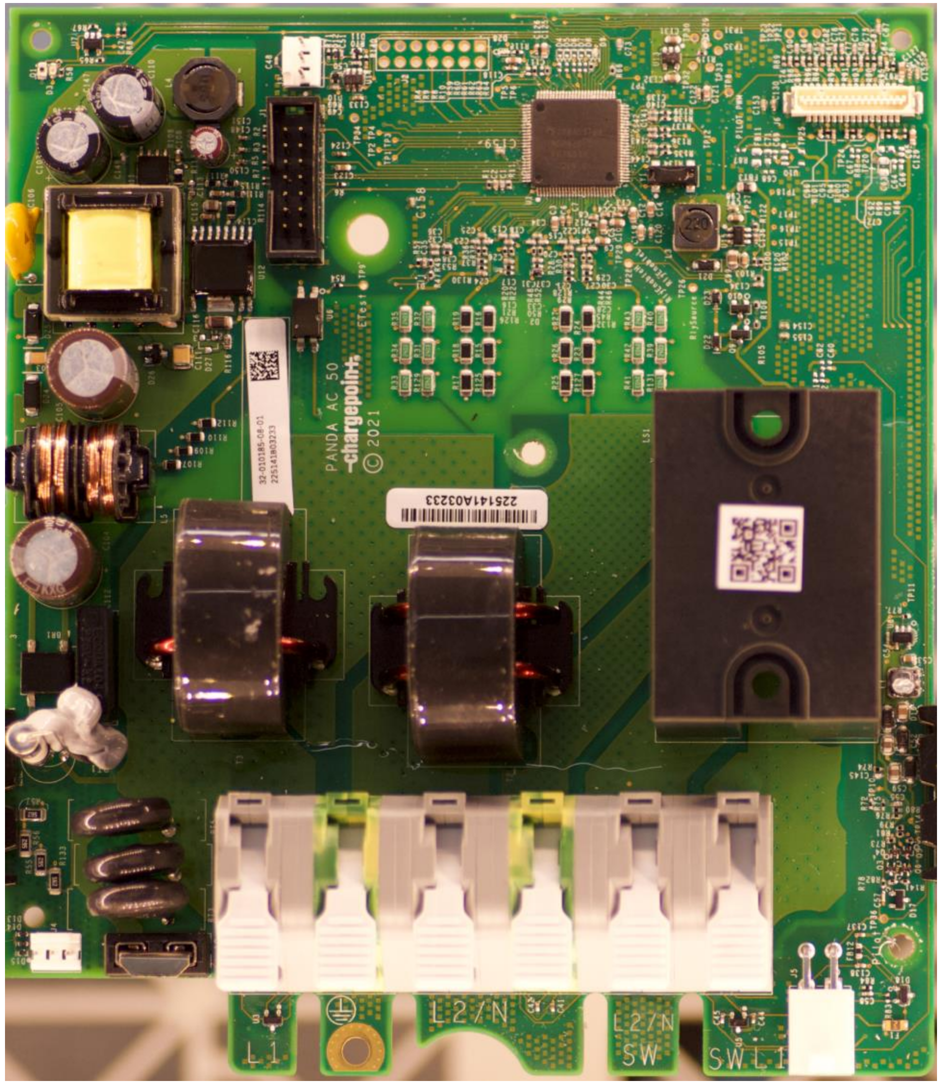
- Atmel AT91SAM9N12
  - OTP bits
  - Secure bootloader
  - JTAG can be disabled
  - OTP writes can be disabled
  - External flash encryption

# ChargePoint Home Flex Metrology



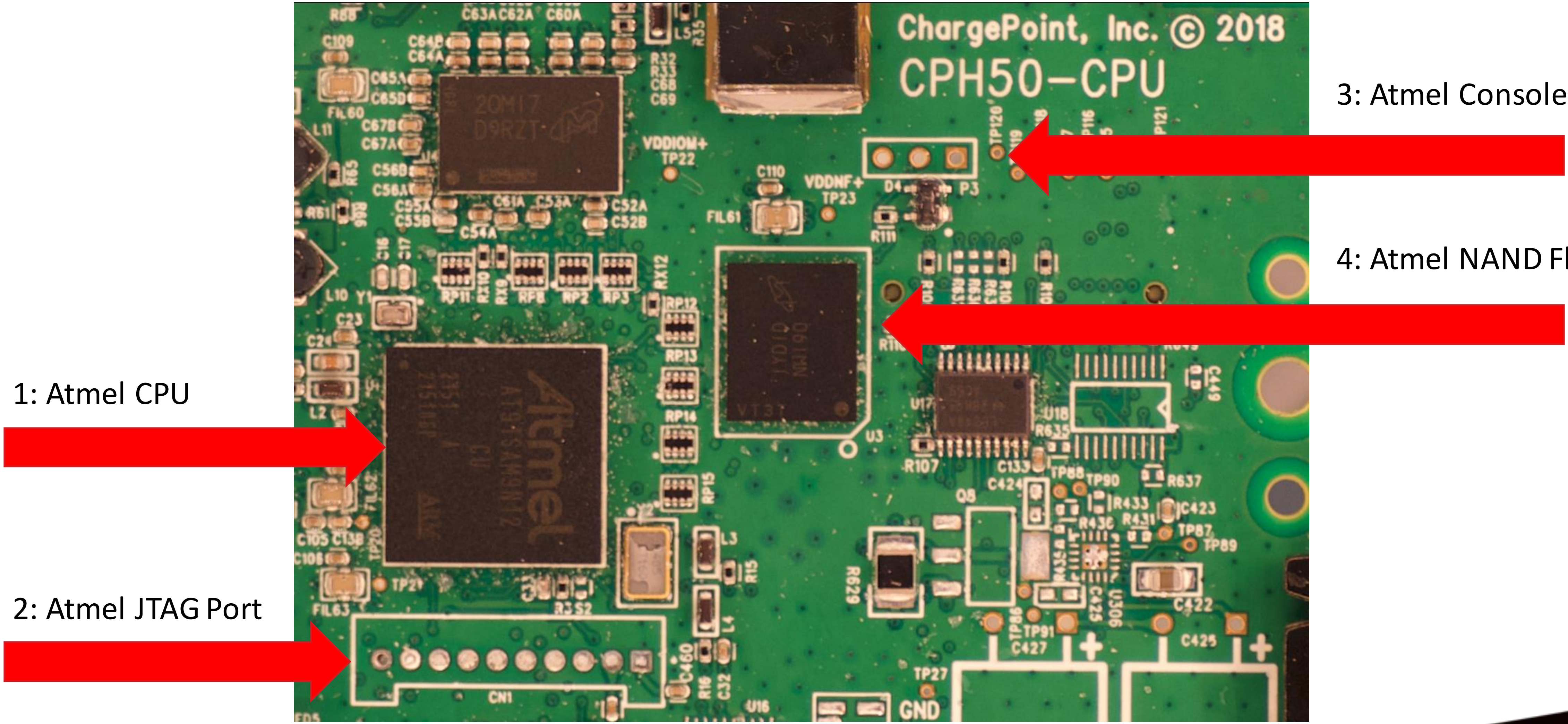
- TI MSP430 F6765 microcontroller
- Exposed interfaces
  - JTAG
  - Serial Console
  - PCB interconnect interface
  - J1772 connector

# ChargePoint Home Flex Metrology Board Available Security Features



- TI MSP430 F6765 microcontroller
  - eFuse (soft)
  - JTAG/SBW debugging locks
    - Bootstrap loader can unlock
  - JTAG can be permanently locked by locking bootstrap loader

# ChargePoint Home Flex CPU Board



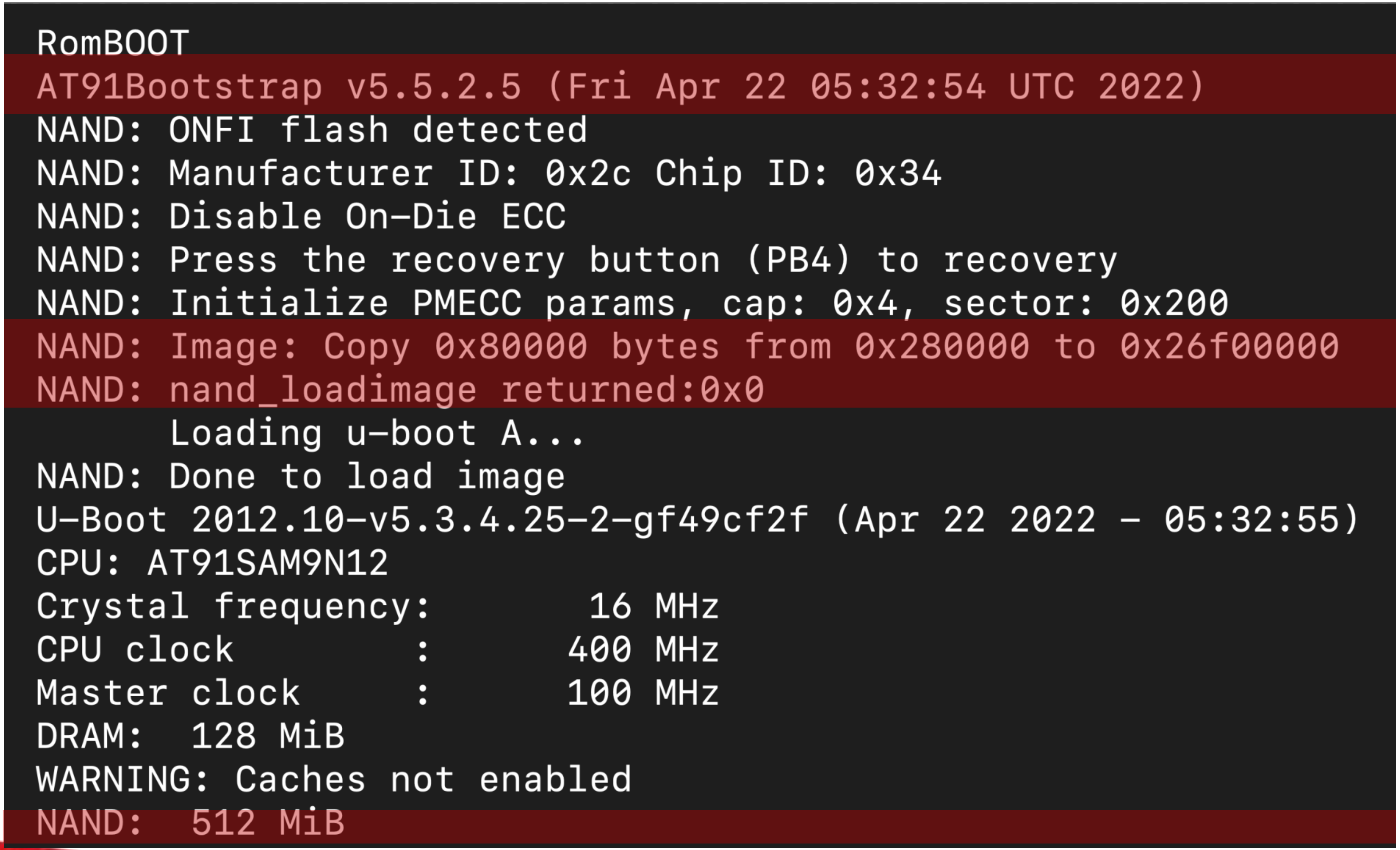
1: Atmel CPU

2: Atmel JTAG Port

3: Atmel Console Port

4: Atmel NAND Flash

# ChargePoint Home Flex - Extracting Flash



```
RomBOOT
AT91Bootstrap v5.5.2.5 (Fri Apr 22 05:32:54 UTC 2022)
NAND: ONFI flash detected
NAND: Manufacturer ID: 0x2c Chip ID: 0x34
NAND: Disable On-Die ECC
NAND: Press the recovery button (PB4) to recovery
NAND: Initialize PMECC params, cap: 0x4, sector: 0x200
NAND: Image: Copy 0x80000 bytes from 0x280000 to 0x26f00000
NAND: nand_loadimage returned:0x0
      Loading u-boot A...
NAND: Done to load image
U-Boot 2012.10-v5.3.4.25-2-gf49cf2f (Apr 22 2022 - 05:32:55)
CPU: AT91SAM9N12
Crystal frequency:       16 MHz
CPU clock        :      400 MHz
Master clock     :      100 MHz
DRAM:  128 MiB
WARNING: Caches not enabled
NAND:  512 MiB
```

## Key Observations

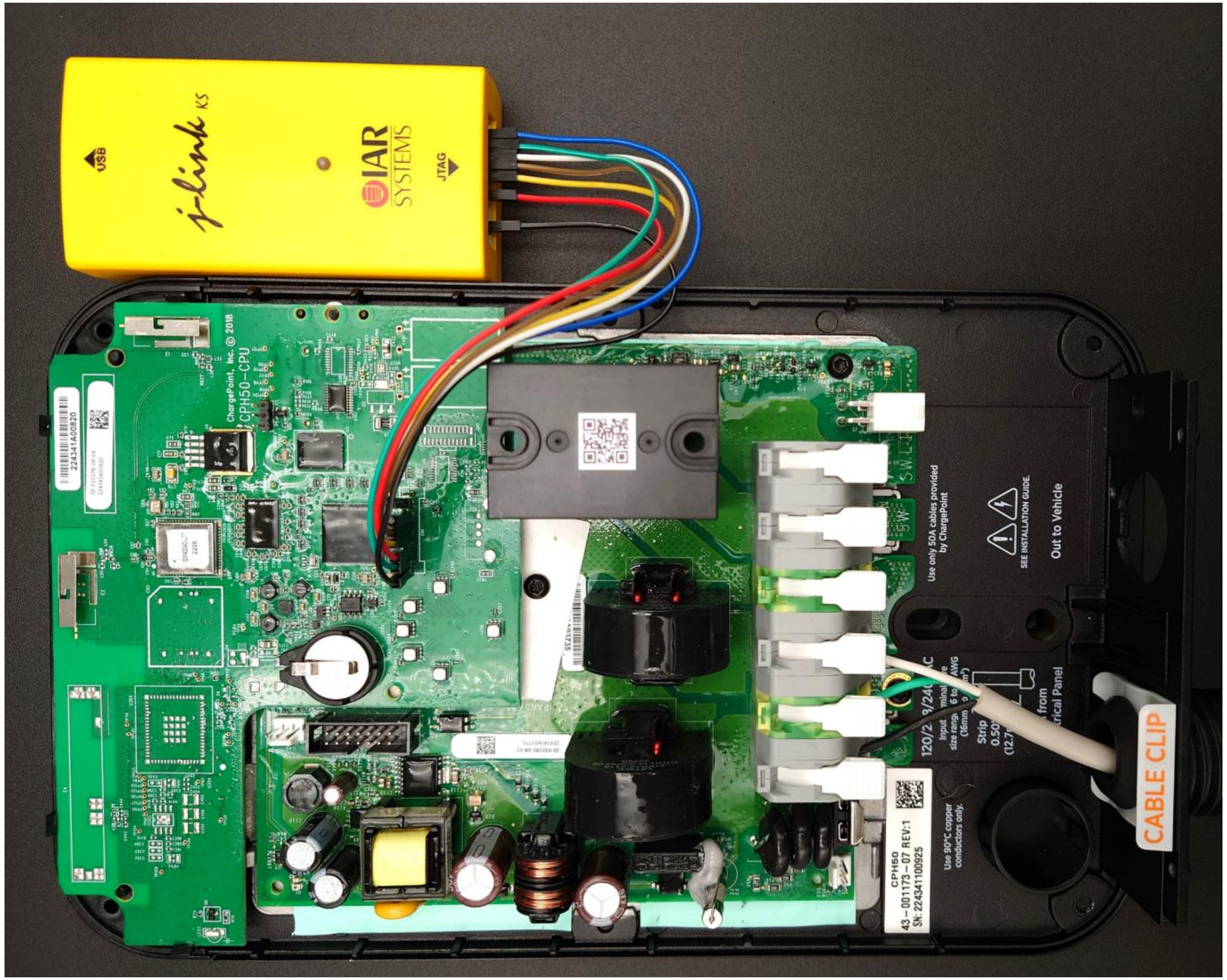
AT91 Bootstrap version

NAND offset for second stage bootloader

Name of function that reads data from NAND (nand_loadimage)

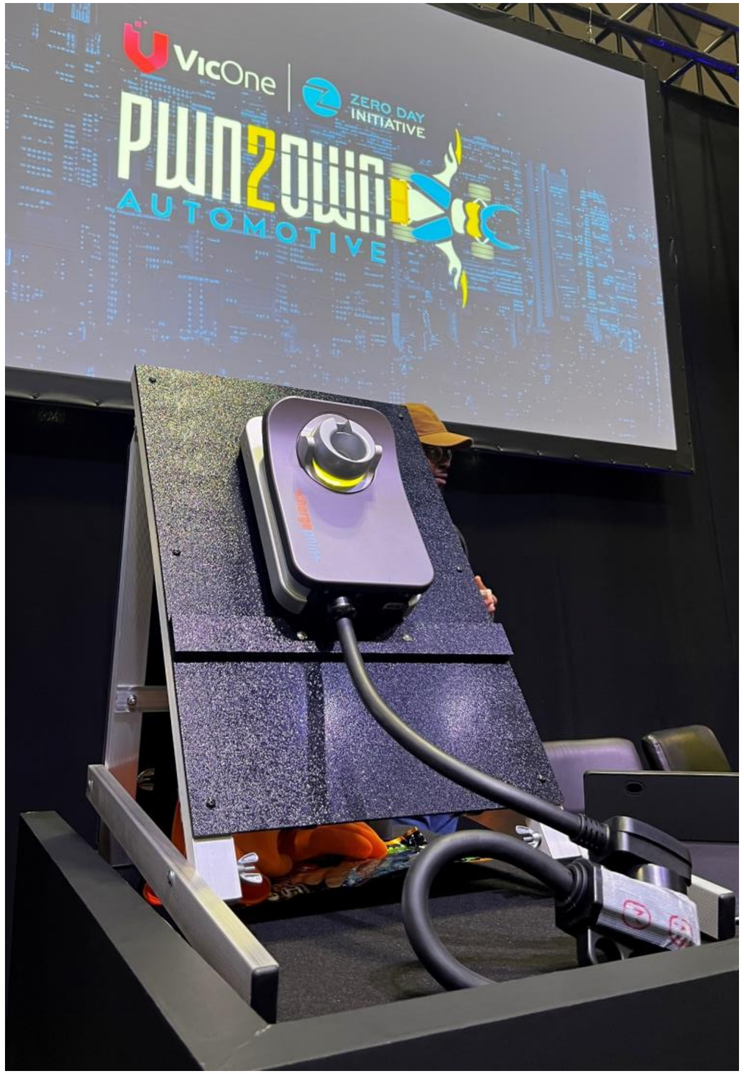
NAND size 512 MB

# ChargePoint Home Flex - Extracting Flash



- Use partition map from serial console to get offsets and lengths to read
- Call nand_loadimage() from AT91BootStrap to read contents of flash into memory
- Save for analysis

# ChargePoint Home Flex in Pwn2Own Automotive 2024



- Number of attempts: 7 total
  - 4 Full Win
  - 3 Success/Collision
- Many exploit chains included multiple bugs
- Most successes involved command injection during the configuration stages of the device
- Bluetooth was the primary vector since it did not require pairing

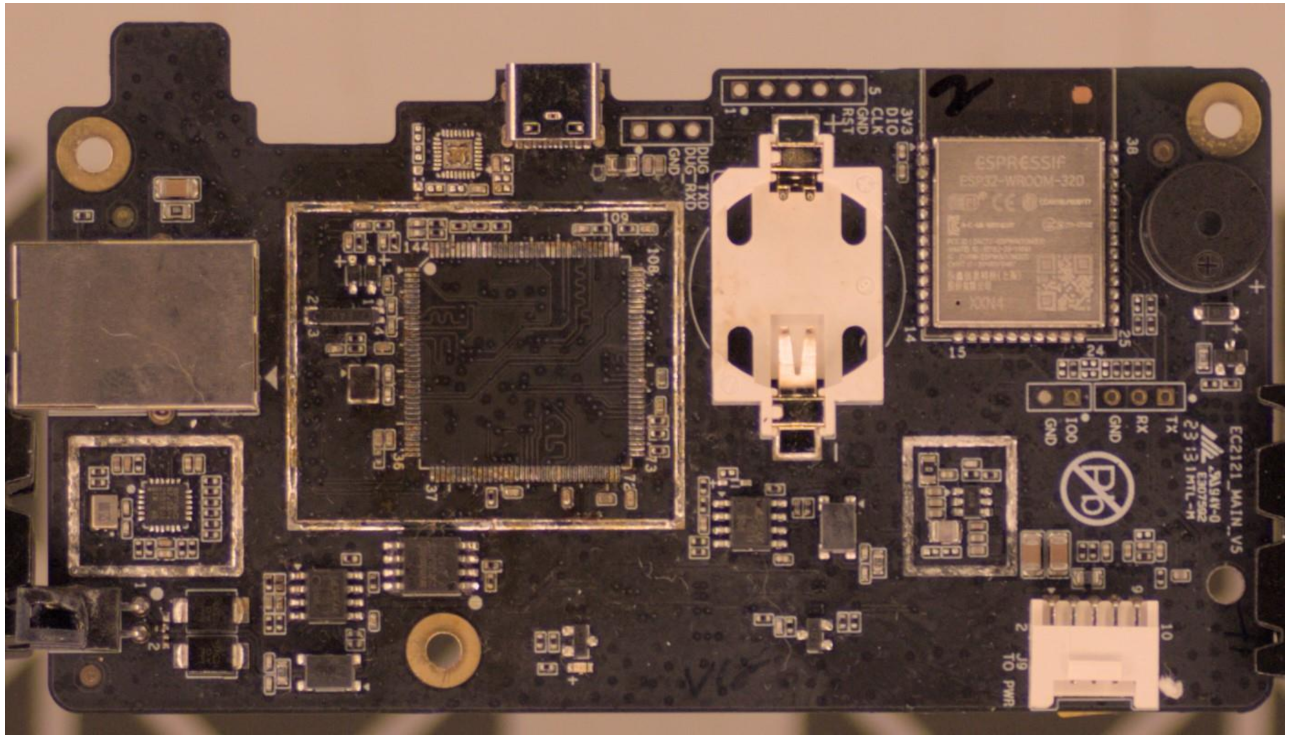
# ChargePoint Home Flex Security Conclusions

- Command injection was predominant bug class
- Lack of BTLE pairing affects security
- Lack of TLS certificate validation in some places

# Autel MaxiCharger

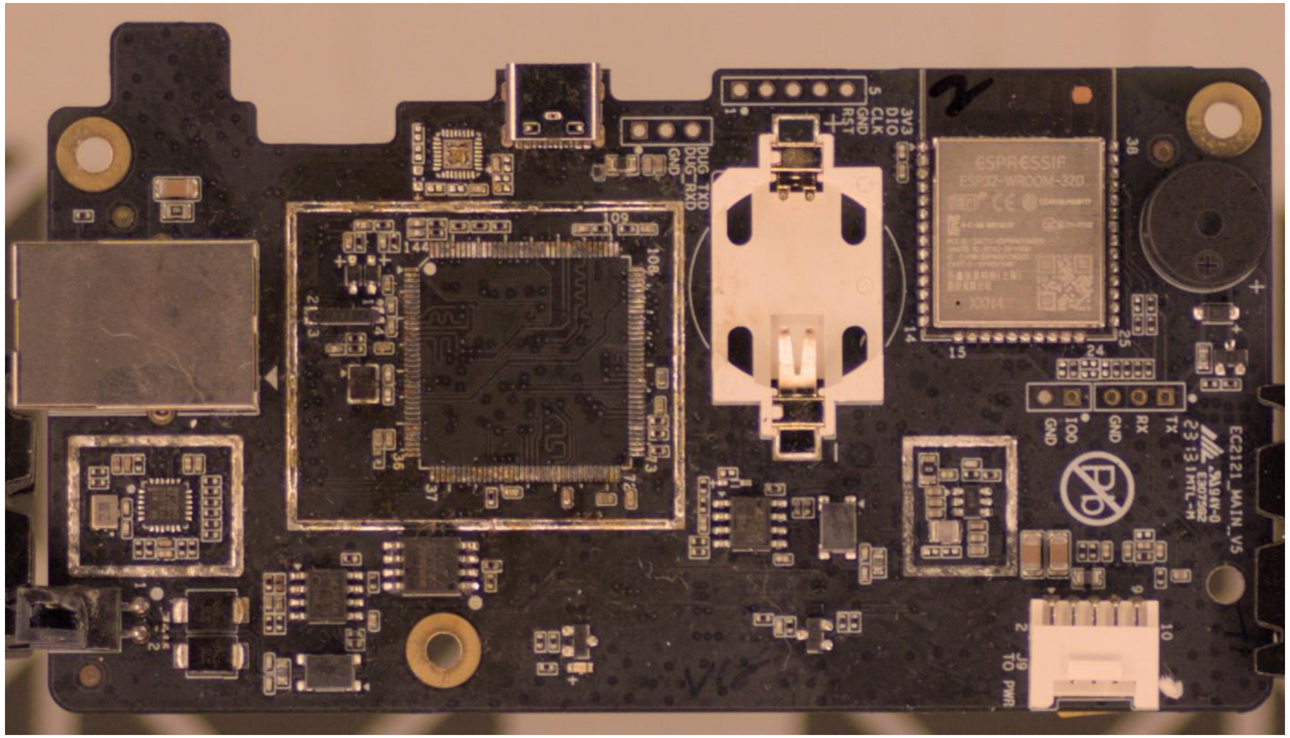
- Multi-PCB design
- CPU Board
  - GigaDevices GD32F407 (ARM Cortex M4)
  - ESP32-WROOM-32D (Xtensa)
- Metrology board
  - ST Micro STM32F407ZGT6 (ARM Cortex M4)
- Mobile Communication Board (LTE)
  - Quectel EC25-AFX

# Autel MaxiCharger CPU Board



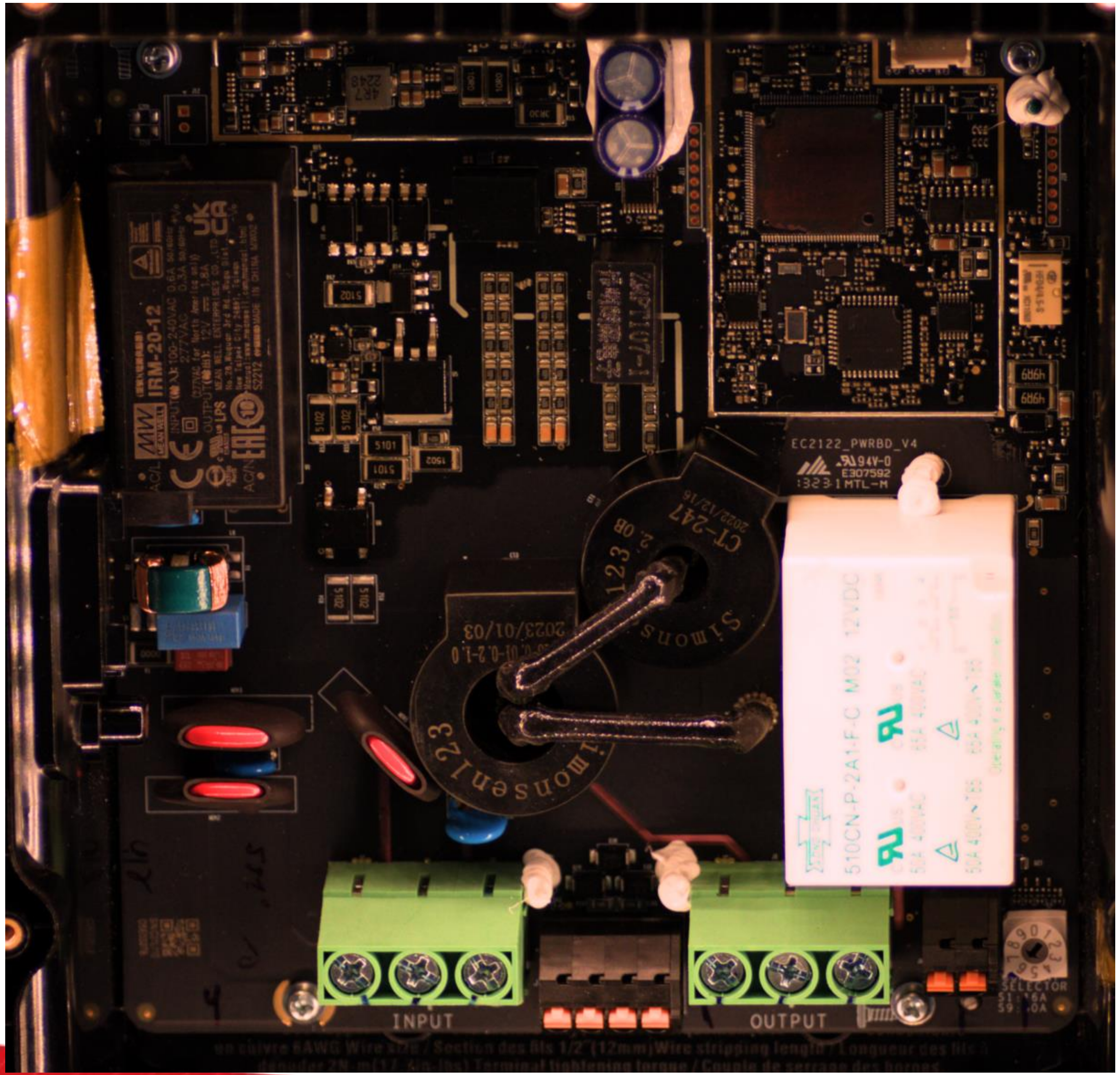
- GigaDevices GD32F407
- ESP-WROOM-32
- Barrot BR8051A01 Bluetooth
- Multiple serial ports emit boot logs for the main CPU and ESP

# Autel MaxiCharger CPU Board Available Security Features



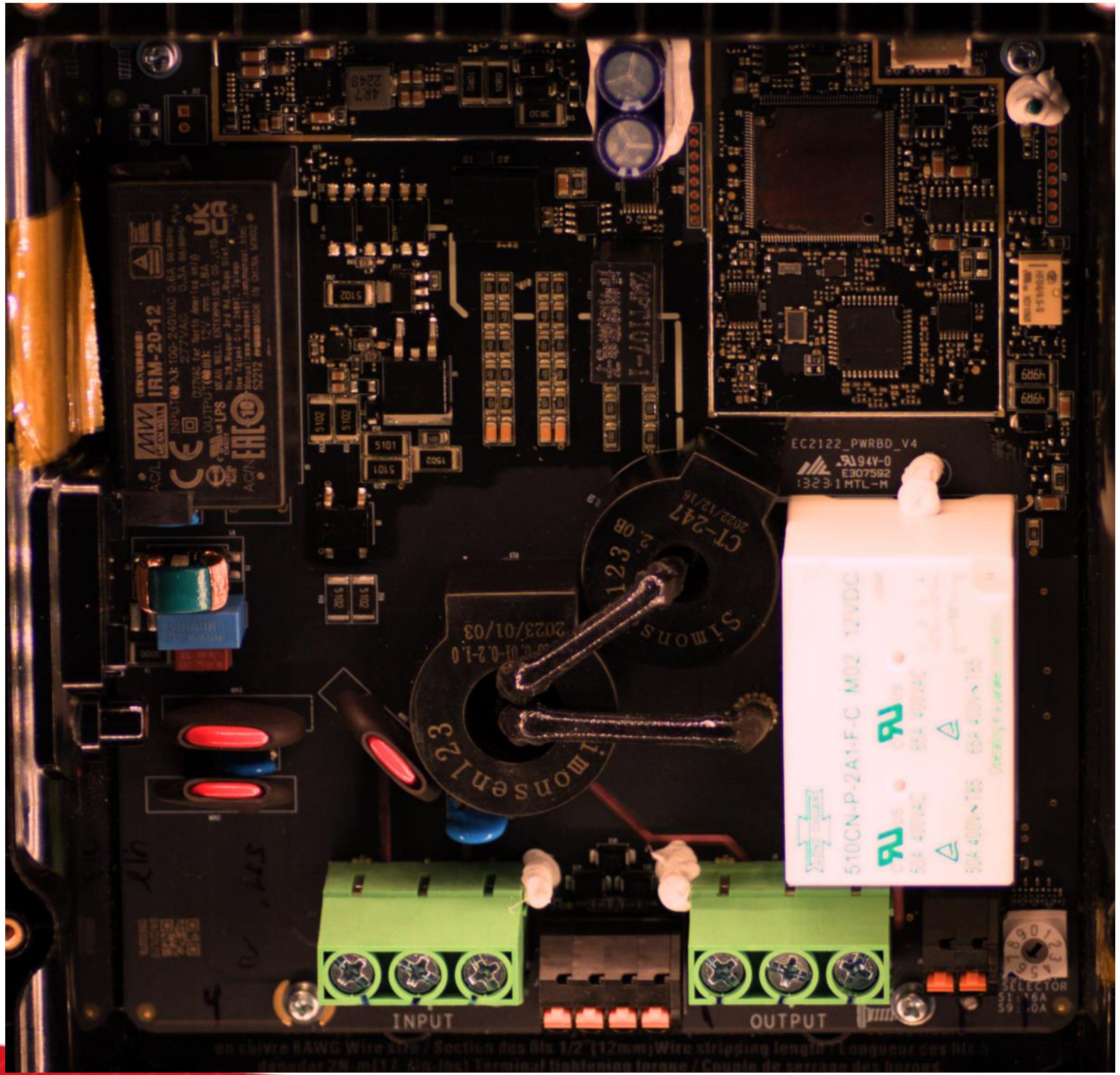
- GigaDevices GD32F407
  - OTP for user features
  - Mutable security features
    - Firmware readout protection was enabled
    - JTAG and firmware access can be disabled
- ESP-WROOM-32
  - Provides OTP to configure security features
  - JTAG can be permanently disabled
  - Supports hardware encryption of RAM and flash
  - Supports glitching detection

# Autel MaxiCharger Metrology Board



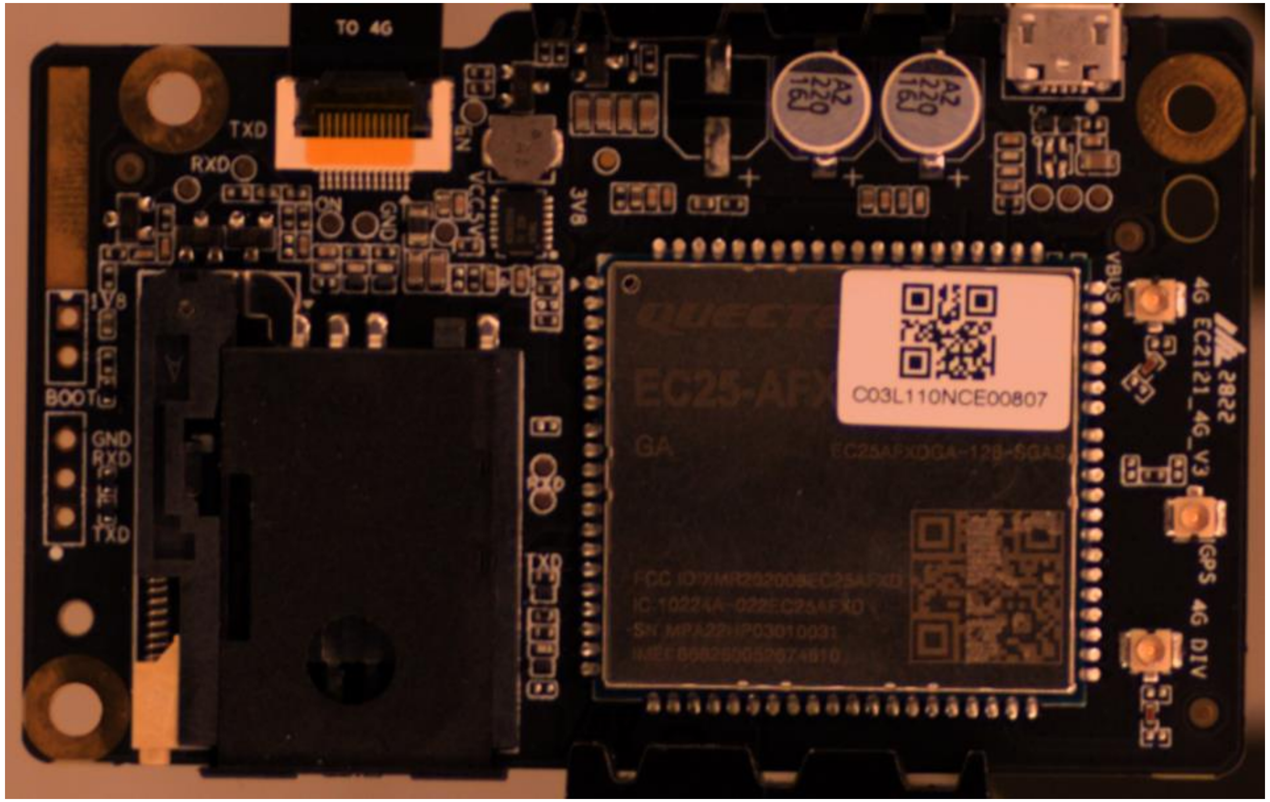
- ST Micro STM32F407ZGT6
- Renergy RN830(B)
- Functional serial port emits boot logs

# Autel MaxiCharger Metrology Board Available Security  Features



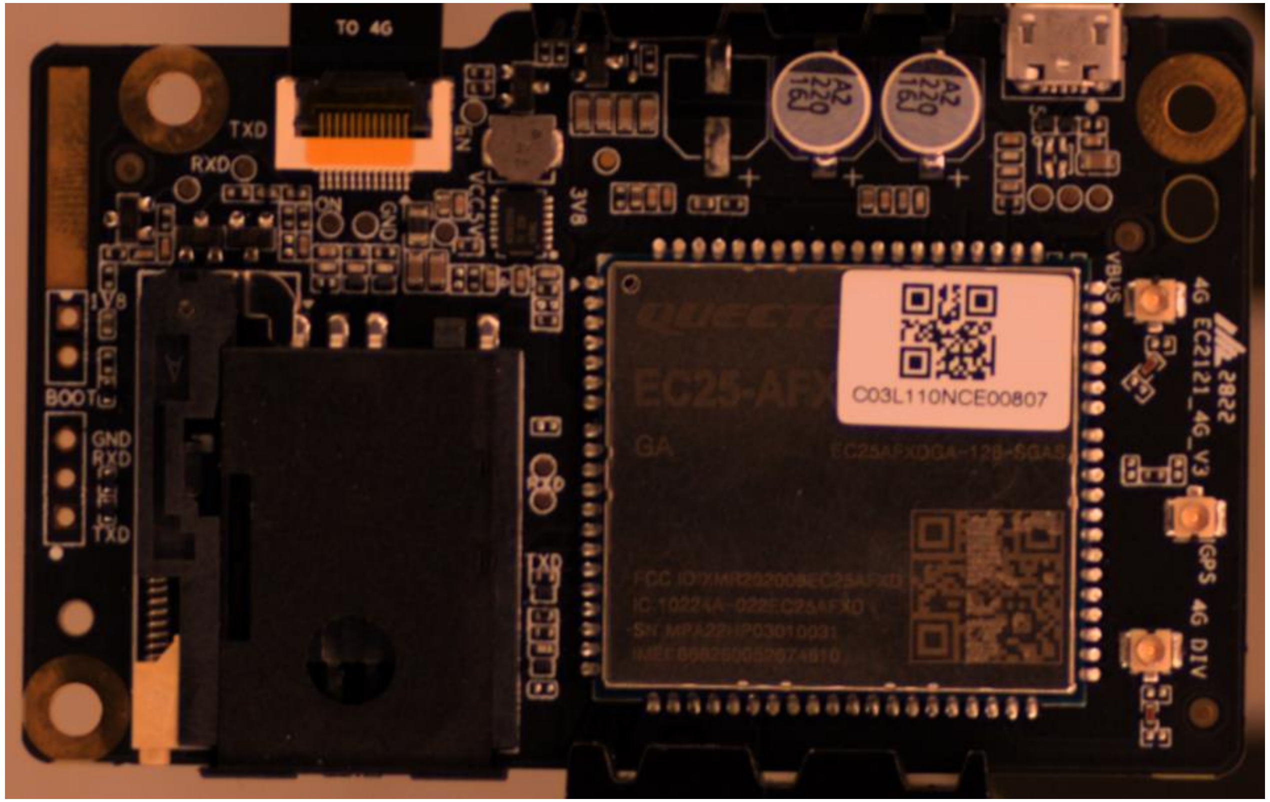
- ST Micro STM32F407ZGT6
  - Similar to the GigaDevices CPU
  - Use of One-time-programmable (OTP) memory to enable security features
  - Firmware readout protection enabled
  - JTAG and firmware access can be permanently disabled
  - Brown-out, clock skew, and glitch detection capabilities

# Autel MaxiCharger Radio Board



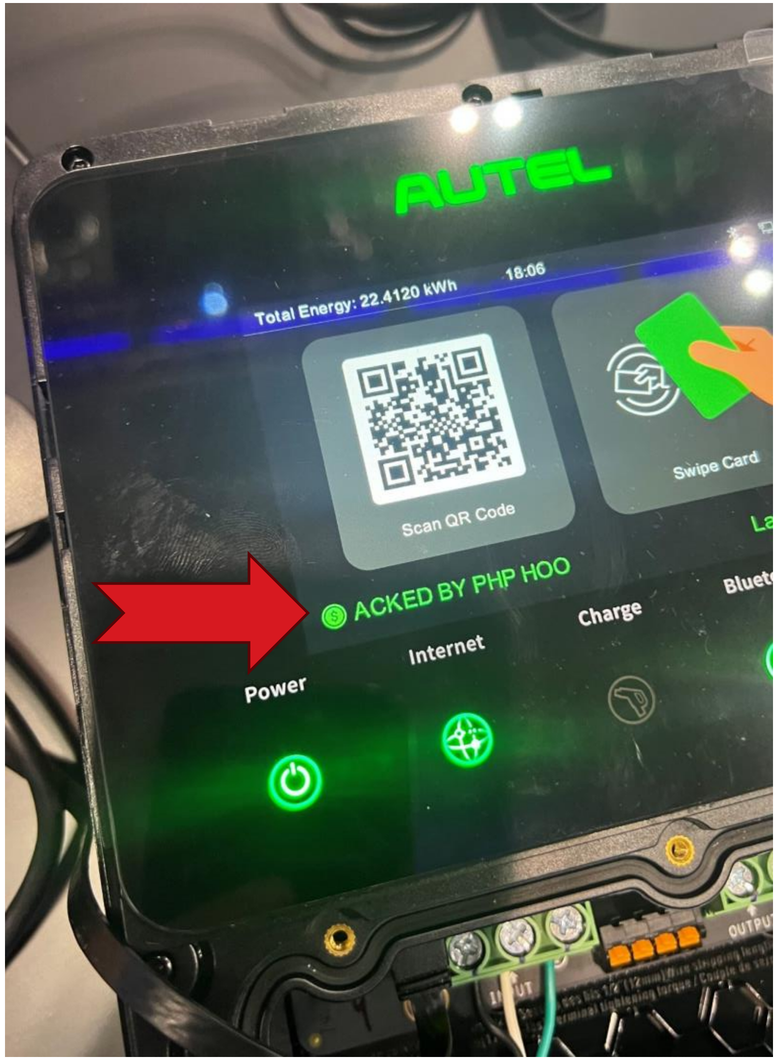
- Mobile communications board
- Quectel EC25-AFX
- Functional serial port emits boot logs
- Similar device is present in Tesla vehicles

# Autel MaxiCharger Radio Board Available Security Features



- Quectel EC25-AFX
  - Secure boot
  - Authenticated debugging

# Autel MaxiCharger in Pwn2Own Automotive 2024



- Number of attempts: 5
  - 2 Full Win
  - 2 Success/Collision
- Most exploit chains included multiple bugs
- All successes were stack buffer overflow exploits and resulted in shell code execution
- Vulnerabilities in Bluetooth and client network handling code

# Autel MaxiCharger Security Conclusions

- Firmware suffers from several discovered stack buffer overflows in multiple features
- Lacks mitigations for stack-based buffer overflows
  - No stack cookies
  - No memory execution protection available
- Hardcoded device credentials

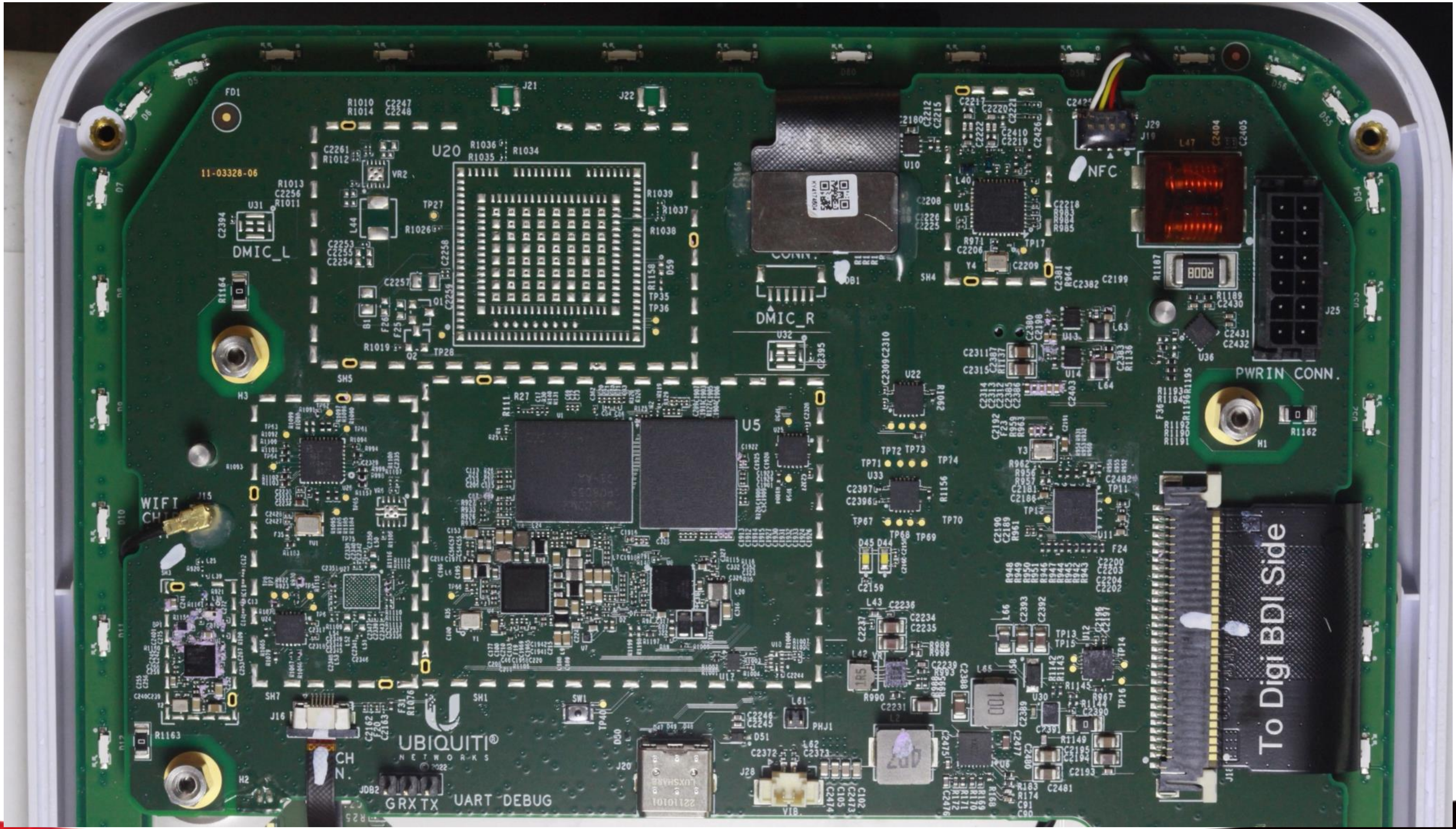
# Ubiquiti EV Station

- Highly integrated design
- CPU Board
  - Android OS
  - Qualcomm APQ8053 SoC (ARM Cortex A53)
  - Nuvoton M482LGCAE (ARM Cortex M4)
  - Qualcomm WCN3680B (Wi-Fi)
  - NXP PN71501 (NFC)
  - UART DEBUG port
  - USB C port

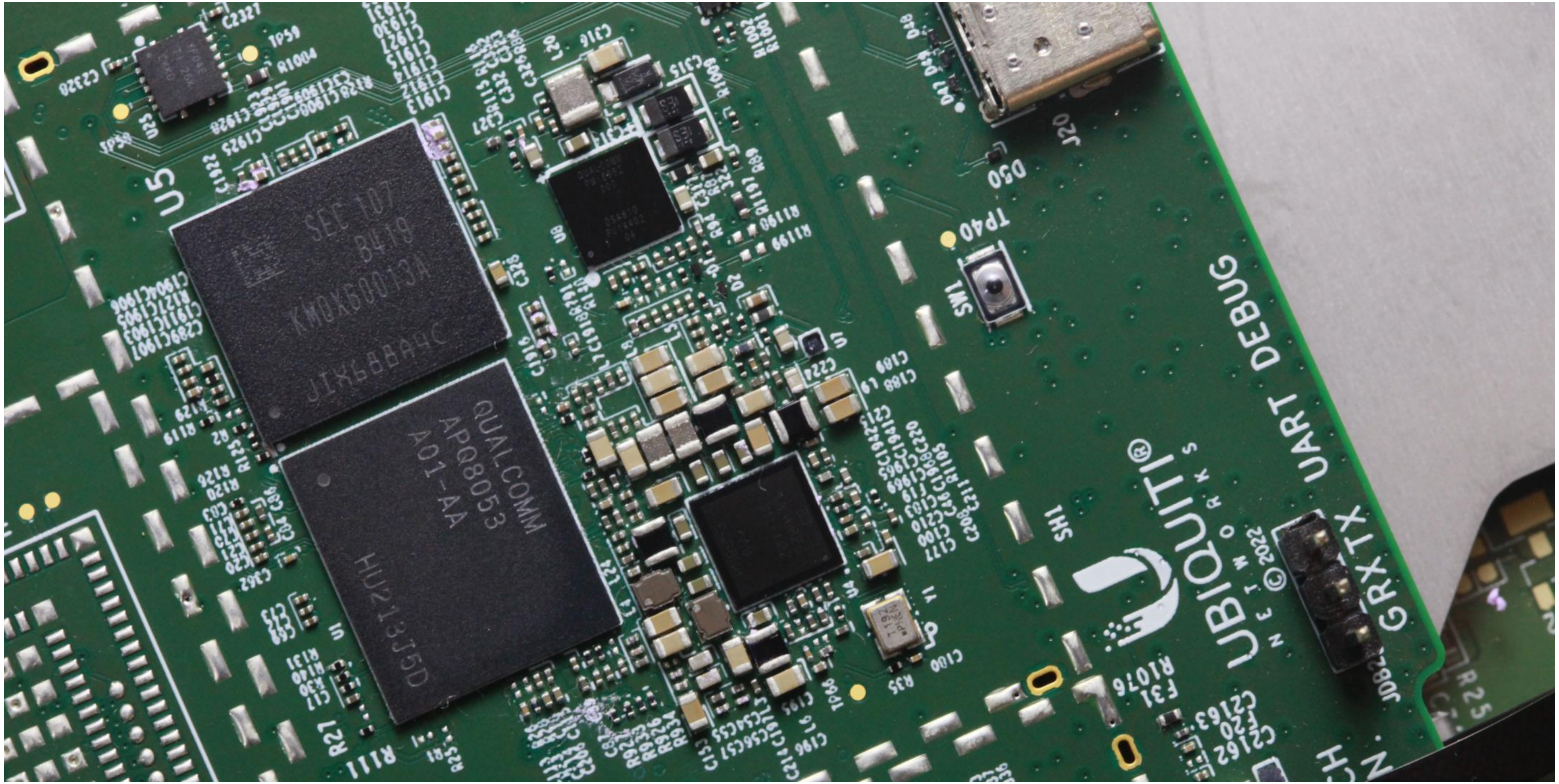
# Ubiquiti EV Station Available Security Features

- Qualcomm APQ8053 SoC (ARM Cortex A53)
  - Public documentation not found
  - Security features from the product brief:
    - Qualcomm Processor Security
    - Qualcomm Device Lock Authentication
    - Qualcomm Content Protection
  - Security features on par with Android devices

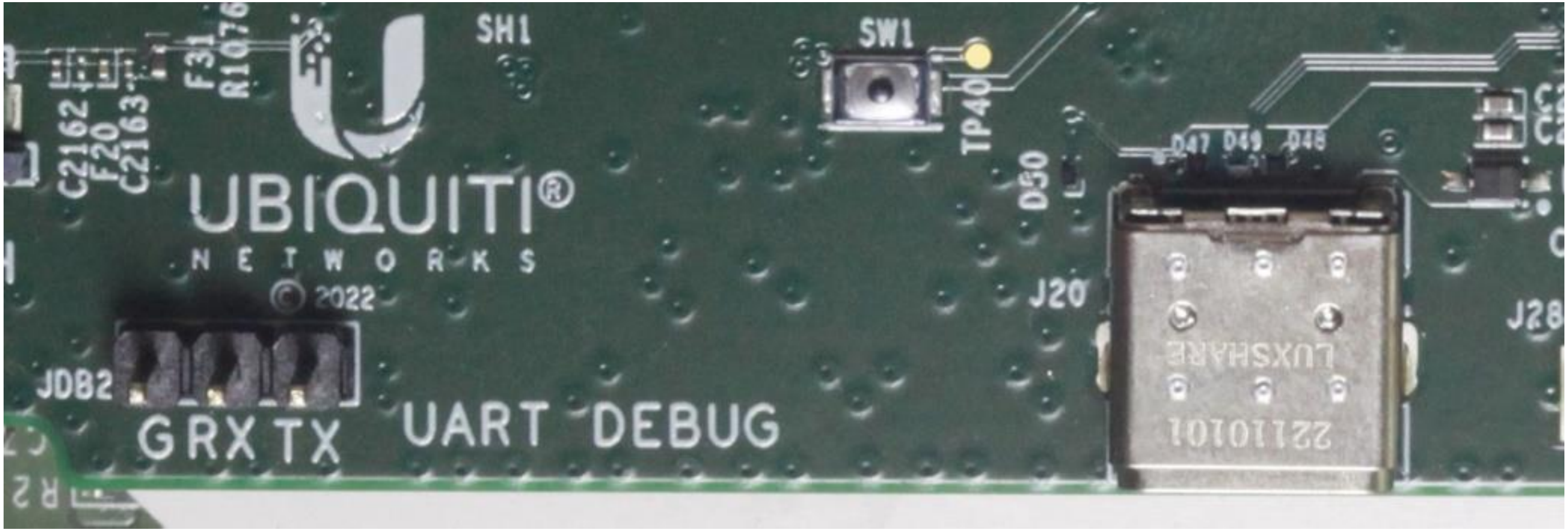
# Ubiquiti EV Station CPU Board



# Ubiquiti EV Station Qualcomm Detail



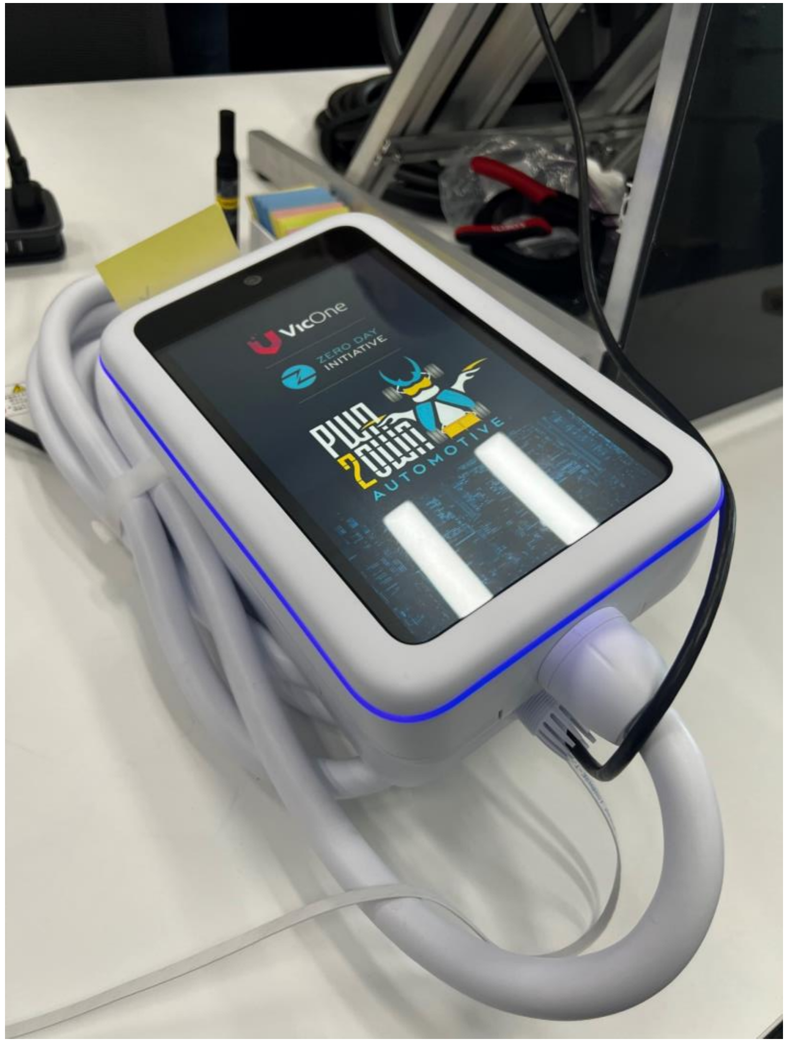
# Ubiquiti EV Station – Serial Console, USBC, Button



# Ubiquiti EV Station

- Android OS
- Serial console enabled
- Ubiquiti have a standard way to enable remote ADB debugging
- Typical deployments use a management console like the Dream Machine

# Ubiquiti EV Station in Pwn2Own Automotive 2024

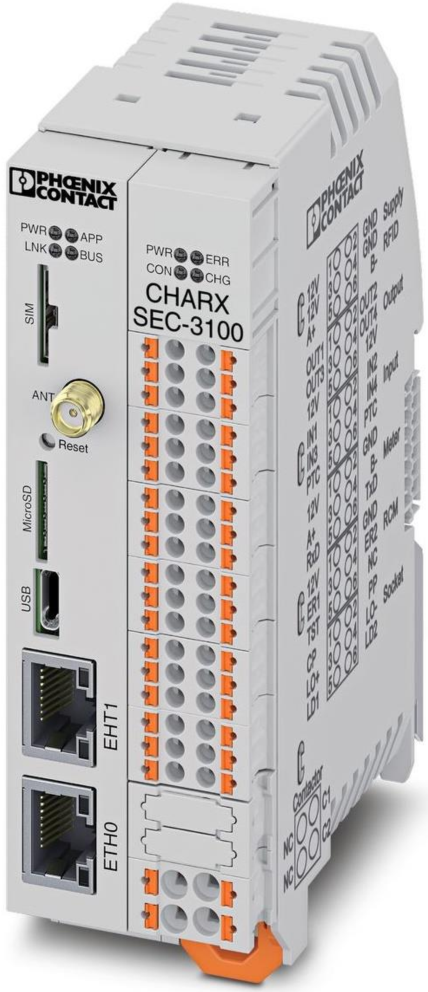


- Number of attempts: 2 total
  - 2 Full Win
  - Both exploits utilized a Wi-Fi path to exploit debug capabilities.
  - The attempts differed somewhat in how they exploited issues with credential checks by the device

# Ubiquiti EV Station Security Conclusions

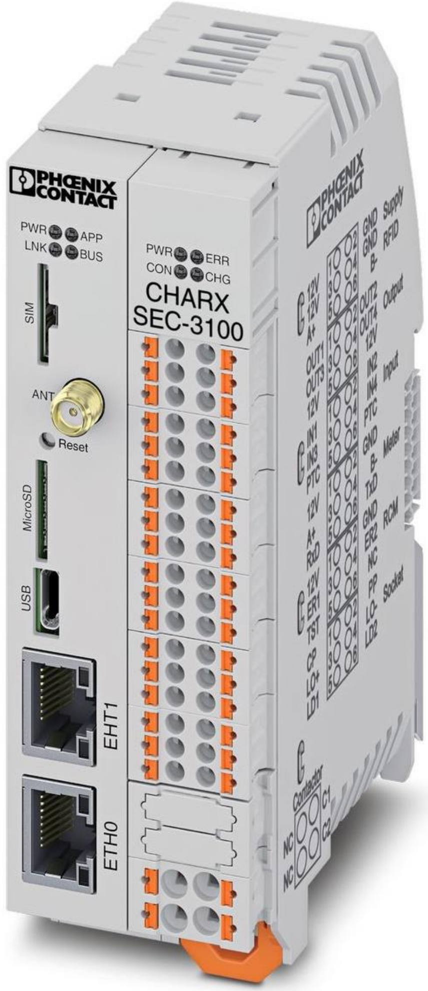
- Mishandling of authentication
- Use of hardcoded credentials
- Lack of TLS certificate authentication when connecting to management console
- Vendor removed debugging system protections

# Phoenix Contact CHARX SEC-3100



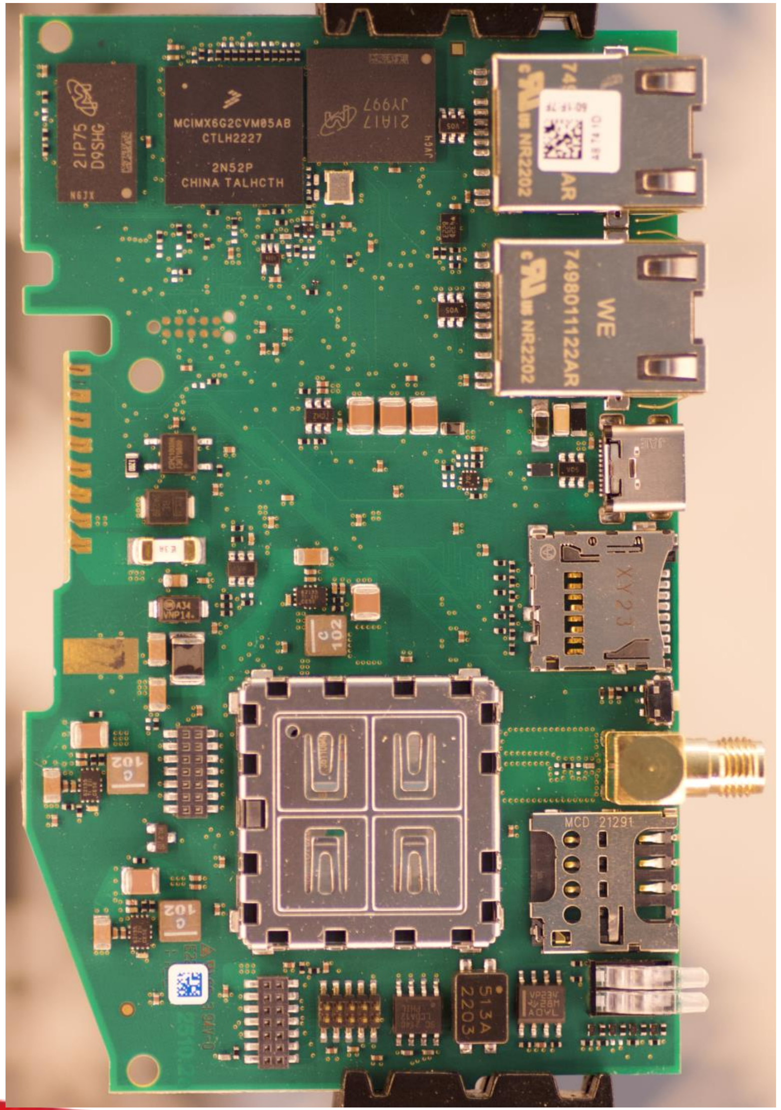
- Dual-PCB Design
- CPU Board
  - NXP i.MX 6UltraLite (ARM Cortex A7)
    - MCIMX6G2CVM05AB
  - Infineon SLB 9670 TPM
  - Linux OS
- Metrology Board
  - Microchip STM32F303 (ARM Cortex M4)

# Phoenix Contact CHARX SEC-3100 Available Security Features



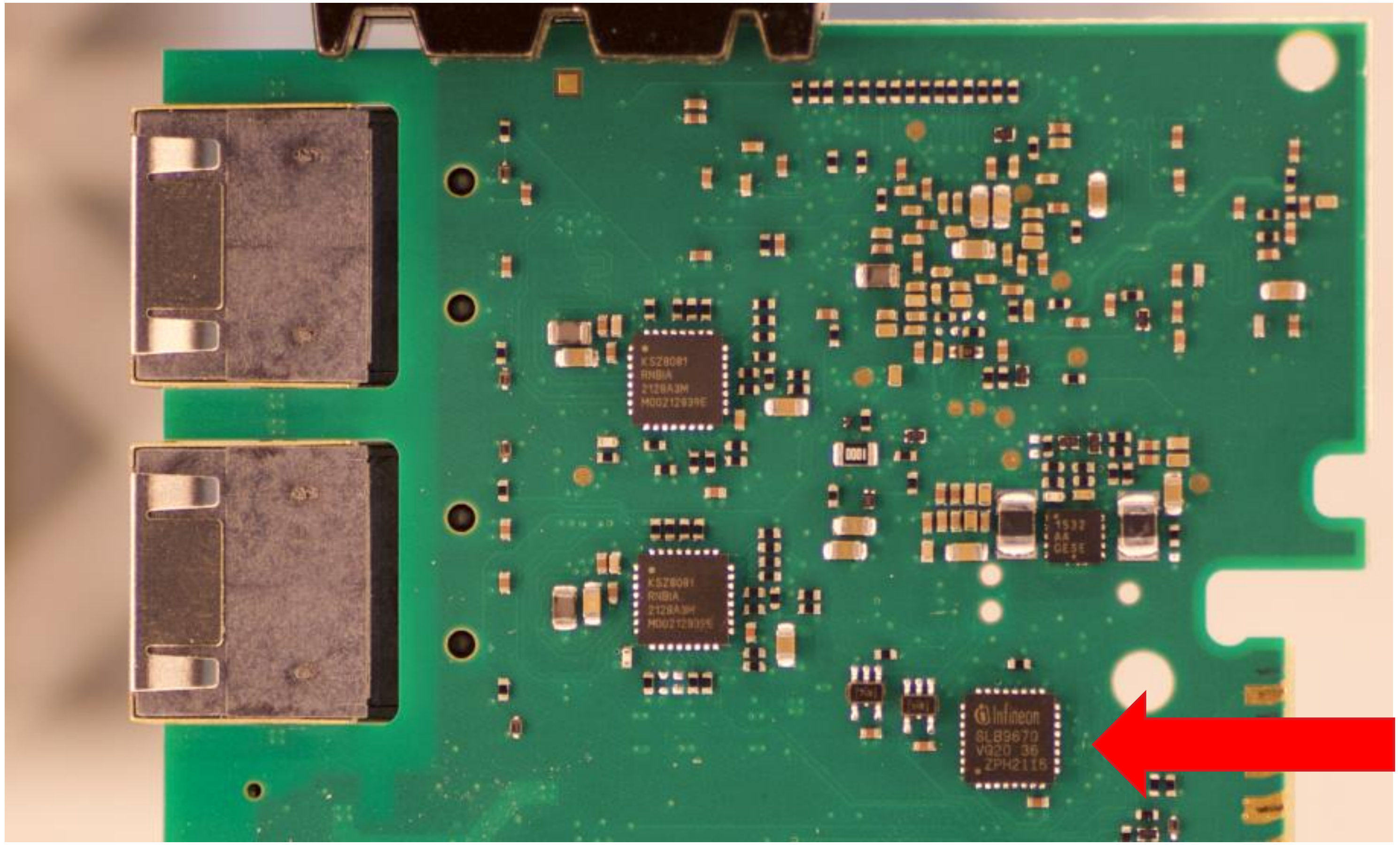
- CPU Board
  - NXP i.MX 6UltraLite
    - SNVS - secure nonvolatile storage
    - High Assurance Boot
    - JTAG security
    - Supports BUS encryption
    - TrustZone
    - Secure RAM
    - OTP
  - Infineon SLB 9670 TPM
    - Appears to be unused

# Phoenix Contact CHARX SEC-3100 CPU Board



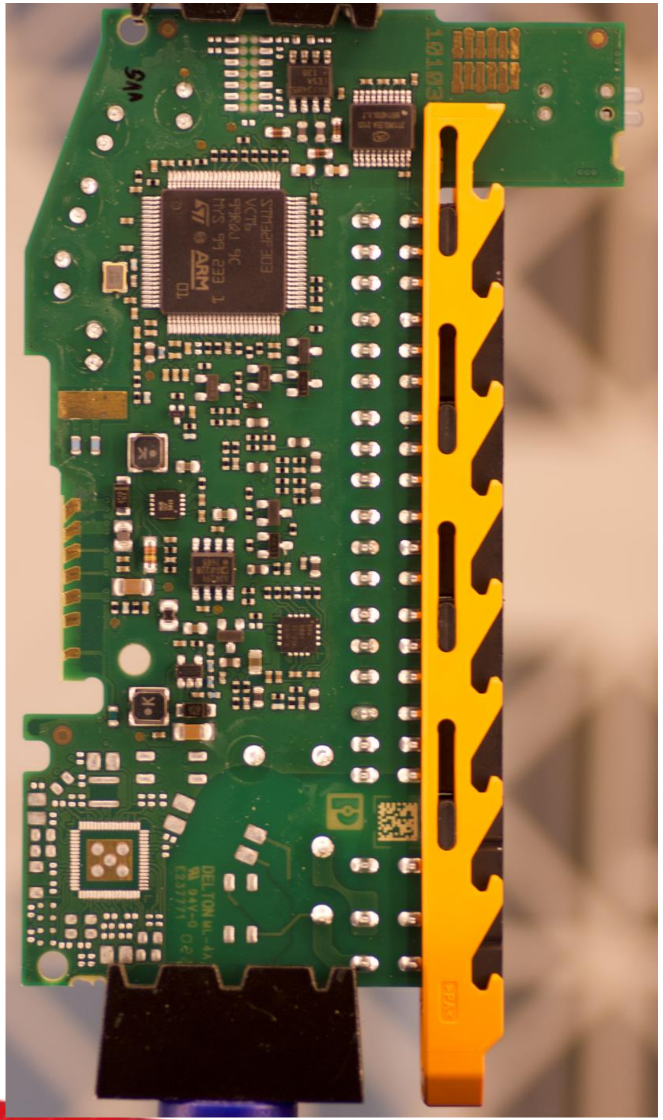
- CPU Board
  - NXP i.MX 6UltraLite ARM
    - MCIMX6G2CVM05AB
  - Infineon SLB 9670 TPM
  - Linux OS

# Phoenix Contact CHARX SEC-3100 CPU Board (Reverse side)



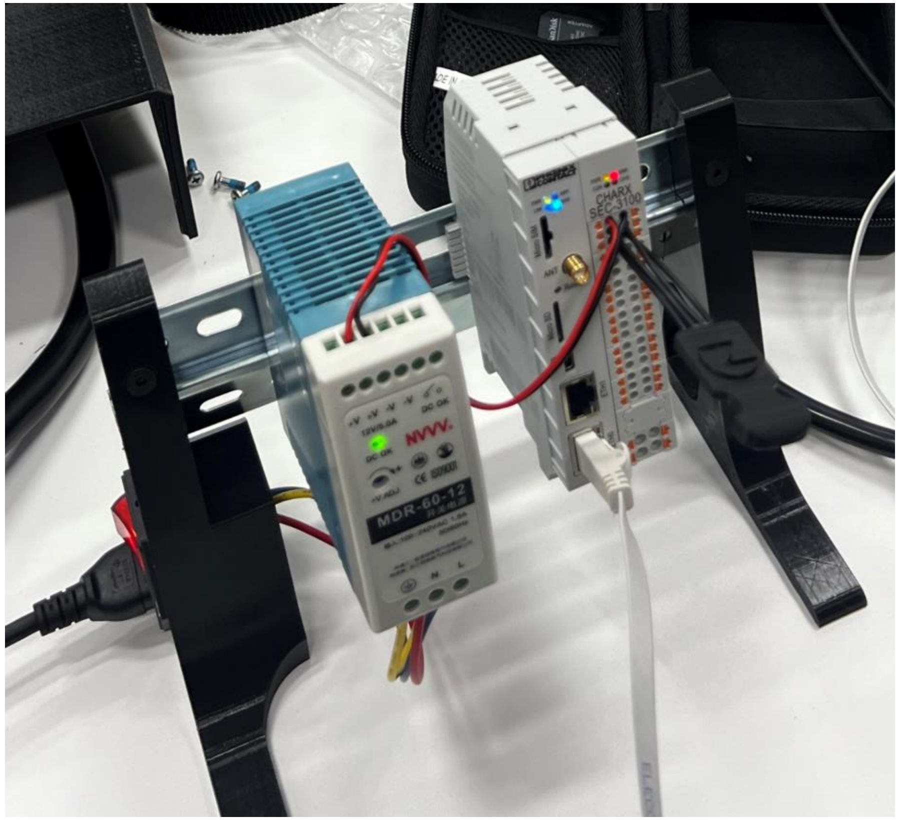
- CPU Board
  - Infineon SLB 9670 TPM
- Doesn’t appear to be in use

# Phoenix Contact CHARX SEC-3100 Metrology Board



- Metrology Board
  - Microchip STM32F303
- Connects to CPU board via a bus connector located in the DIN rail

# Phoenix Contact CHARX SEC-3100 in Pwn2Own Automotive 2024



- Number of attempts: 8 total
  - 3 Full Win
  - 2 Success/Collision
- Many exploit chains included multiple bugs
- Exploits had significant variability relative to the exploits of the other chargers
- Vulnerabilities in various services (PPPD, OCPP, MQTT) were utilized
- Privilege separation required escalation

# Phoenix Contact CHARX SEC-3100 Security Conclusions

- Software uses ASLR
  - Some inter-library relative offsets are preserved
- Use-after-free vulnerability
- Command injection vulnerabilities
- Vulnerabilities in protocol parsing
- Firewall configuration allows bypasses
- File upload vulnerabilities
- Multiple local privilege escalation bugs

# Pwn2Own Automotive 2024 Overall Conclusions

- Debug access easily available
  - Serial
  - JTAG, SWD, SBW, ADB debug
  - Special network services with complete device control
- Device designs don’t include secure chip variants, or don’t employ security features in the chips being used
- Devices that have support for TPM and TEE (TrustZone) appear unused
- Most devices don’t employ secure boot
- Chargers don’t employ hardware-backed firmware encryption
  - One instance of signed firmware was observed

# Pwn2Own Automotive 2024 Overall Conclusions

- Parser implementations that contain buffer overflows
- Protocol handlers that allow for command injections
  - Use of system()/popen() calls that don’t sanitize input
- Use of hardcoded credentials
- Code lacking stack cookies
- Code lacking non-execute permissions on stack and heap memory (NX)
- Code lacking ASLR
- ASLR implementations that preserve relative memory layout

# Pwn2Own Automotive 2024 Observed Security Strengths

- Some devices employ secure chip variants with higher security features
  - OTP / Secure boot / JTAG disable / Flash read protection / Flash encryption
  - TPM / TEE / TrustZone hardware on board
- One instance of HW Flash readback protection (but bypassed via V-FI)
- OTA / Automatic updates / Signed updates
- Frequent use of secure network transports TLS/SSH w/cert validation
- Some devices had memory protections
  - Stack cookies, NX protections, ASLR

# Pwn2Own Automotive 2024 Overall Conclusions

- Additional mitigations are required for consumers that deploy these devices to their network
  - Network segmentation / VLANs
  - Additional network firewalling / Traffic filtering
- Many opportunities for improvement
  - Hardware design
  - Software security mitigations
  - Implement SDLC

# Pwn2Own Automotive 2024 Vendor Recommendations

- Employ basic security best practices in:
  - Authentication, input sanitization, use of available mitigations
- Perform static code analysis
- Perform fuzz testing
- Select chips that have memory protection features
  - Employ available security features of chips
  - Firmware encryption doesn’t fix exposed bugs and hinders research
- Use third party audits / bug bounties / engage researcher community / consultants

# Possible impacts of EV charger vulnerabilities

- Steal power
- Confidential data exfiltration
- Backdoor firmware in the device to impact charger functions
- Use charger computing resources for attacker purposes
- Overcharging or undercharging of vehicles
- Trip breakers and cause power to be unavailable
- Create instability in the power grid
- Facilitate attacks against EV charger cloud environment
- Facilitate attacks against other EV chargers in local environment
- Potential to pivot through cloud environment to remote EV chargers

# Trend Micro Blog QRs

- A Detailed Look At Pwn2Own Automotive EV Charger Hardware
- How To: Modifying EV Chargers For Benchtop Experiments
- Looking At The ChargePoint Home Flex Threat Landscape
- Attack Surface Of The Ubiquiti Connect EV Station

# Trend Micro Blog Links

- A Detailed Look At Pwn2Own Automotive EV Charger Hardware
  - https://www.zerodayinitiative.com/blog/2023/11/28/a-detailed-look-at-pwn2own-automotive-ev-charger-hardware
- How To: Modifying EV Chargers For Benchtop Experiments
  - https://www.zerodayinitiative.com/blog/2023/11/8/how-to-modifying-ev-chargers-for-benchtop-experiments
- Looking At The ChargePoint Home Flex Threat Landscape
  - https://www.zerodayinitiative.com/blog/2023/9/7/looking-at-the-chargepoint-home-flex-threat-landscape
- Attack Surface Of The Ubiquiti Connect EV Station
  - https://www.zerodayinitiative.com/blog/2023/12/5/attack-surface-of-the-ubiquiti-connect-ev-station

# Future

Fault Injection (V-FI / EM-FI) was used by contestants

- ChipWhisperer Nano (V-FI)
  - Our glitcher is up and running
  - $50 + JTAG device
- ChipShouter Pico (EM-FI)
  - Free PCB! - $90 in parts
  - Digikey: https://www.digikey.com/short/pv7nd2vf
  - Mouser: https://www.mouser.com/ProjectManager/ProjectDetail.aspx?AccessID=62cd0f8bd2

# Connect With Us Online

www https://www.zerodayinitiative.com

@thezdi, @thezdibugs
@dustin_childs

@thezdi

▶ https://www.youtube.com/c/ZeroDayInitiative

PGP https://www.zerodayinitiative.com/documents/zdi-pgp-key.asc
Fingerprint: 743F 60DB 46EA C4A0 1F7D B545 8088 FEDF 9A5F D228

TREND MICRO™ | Global Leader in Cybersecurity