**Deliverable #6: Device Setup and Port Scanning**

**Project: IoT Vulnerability Research Project**

**Participants:**

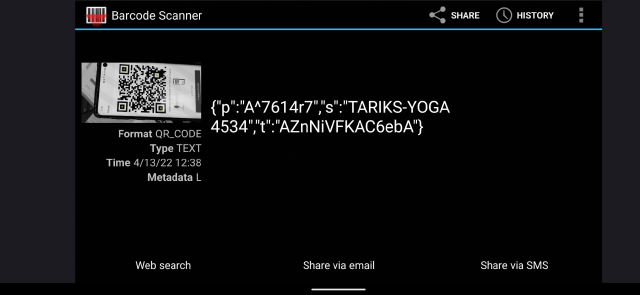
* Vikram Kher
* Varin Jaggi
* Tarik Wilkinson
* Patrick Kakooza
* Liza Moody
* Haoda Wang

**Introduction:**

For this deliverable, we first used wireshark to identify the data that the camera sends out and the data it receives. This also helped us identify the different IP addresses the camera was sending data to and the camera’s own IP address. We then used nmap intense to scan the different ports on the camera and identify which of these are open and which of these are closed. This will help us focus on those ports on the camera which are open and thereby vulnerable to attack.

**Network connection method for camera:**

We used a hotspot to connect to the camera with the app. The camera scans a QR code which allows it to connect to the network. The following picture shows the decoded QR code, which contains a simple JSON with an unencrypted password.



**Nmap Intense + UDP scan output:**

* Key takeaways are that the device is using Linux 2.6.32 - 3.10, an extremely old and vulnerable version
* We can use this information to find vulnerabilities in these old versions of linux.
* One of the UDP ports it found was a “NetworkVideoTransmitter” port

Raw output:

vikramkher@Vikrams-MBP ~ % sudo nmap -sS -sU -T4 -A -v 192.168.137.227

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-13 12:57 PDT

NSE: Loaded 155 scripts for scanning.

NSE: Script Pre-scanning.

Initiating NSE at 12:57

Completed NSE at 12:57, 0.00s elapsed

Initiating NSE at 12:57

Completed NSE at 12:57, 0.00s elapsed

Initiating NSE at 12:57

Completed NSE at 12:57, 0.00s elapsed

Initiating ARP Ping Scan at 12:57

Scanning 192.168.137.227 [1 port]

Completed ARP Ping Scan at 12:57, 0.10s elapsed (1 total hosts)

Initiating Parallel DNS resolution of 1 host. at 12:57

Completed Parallel DNS resolution of 1 host. at 12:57, 0.04s elapsed

Initiating SYN Stealth Scan at 12:57

Scanning 101207387.mshome.net (192.168.137.227) [1000 ports]

Discovered open port 6668/tcp on 192.168.137.227

Completed SYN Stealth Scan at 12:57, 0.83s elapsed (1000 total ports)

Initiating UDP Scan at 12:57

Scanning 101207387.mshome.net (192.168.137.227) [1000 ports]

Increasing send delay for 192.168.137.227 from 0 to 50 due to 11 out of 19 dropped probes since last increase.

Increasing send delay for 192.168.137.227 from 50 to 100 due to max\_successful\_tryno increase to 5

Increasing send delay for 192.168.137.227 from 100 to 200 due to max\_successful\_tryno increase to 6

Warning: 192.168.137.227 giving up on port because retransmission cap hit (6).

UDP Scan Timing: About 10.73% done; ETC: 13:02 (0:04:18 remaining)

Increasing send delay for 192.168.137.227 from 200 to 400 due to 11 out of 11 dropped probes since last increase.

Increasing send delay for 192.168.137.227 from 400 to 800 due to 11 out of 12 dropped probes since last increase.

UDP Scan Timing: About 13.86% done; ETC: 13:04 (0:06:19 remaining)

UDP Scan Timing: About 16.83% done; ETC: 13:06 (0:07:30 remaining)

UDP Scan Timing: About 20.09% done; ETC: 13:07 (0:08:01 remaining)

UDP Scan Timing: About 25.11% done; ETC: 13:09 (0:08:33 remaining)

UDP Scan Timing: About 39.09% done; ETC: 13:10 (0:07:58 remaining)

UDP Scan Timing: About 48.83% done; ETC: 13:11 (0:07:18 remaining)

UDP Scan Timing: About 54.87% done; ETC: 13:12 (0:06:33 remaining)

UDP Scan Timing: About 60.39% done; ETC: 13:12 (0:05:49 remaining)

UDP Scan Timing: About 65.94% done; ETC: 13:12 (0:05:04 remaining)

UDP Scan Timing: About 71.66% done; ETC: 13:12 (0:04:17 remaining)

UDP Scan Timing: About 77.09% done; ETC: 13:12 (0:03:31 remaining)

UDP Scan Timing: About 82.27% done; ETC: 13:13 (0:02:44 remaining)

UDP Scan Timing: About 87.36% done; ETC: 13:13 (0:01:57 remaining)

UDP Scan Timing: About 92.47% done; ETC: 13:13 (0:01:10 remaining)

Discovered open port 3702/udp on 192.168.137.227

Discovered open port 3703/udp on 192.168.137.227

Completed UDP Scan at 13:13, 978.96s elapsed (1000 total ports)

Initiating Service scan at 13:13

Scanning 54 services on 101207387.mshome.net (192.168.137.227)

Service scan Timing: About 5.56% done; ETC: 13:29 (0:14:27 remaining)

Service scan Timing: About 12.96% done; ETC: 13:24 (0:09:04 remaining)

Service scan Timing: About 61.11% done; ETC: 13:17 (0:01:14 remaining)

Service scan Timing: About 74.07% done; ETC: 13:17 (0:00:56 remaining)

Completed Service scan at 13:16, 175.20s elapsed (54 services on 1 host)

Initiating OS detection (try #1) against 101207387.mshome.net (192.168.137.227)

NSE: Script scanning 192.168.137.227.

Initiating NSE at 13:16

Completed NSE at 13:18, 121.45s elapsed

Initiating NSE at 13:18

Completed NSE at 13:18, 1.03s elapsed

Initiating NSE at 13:18

Completed NSE at 13:18, 0.01s elapsed

Nmap scan report for 101207387.mshome.net (192.168.137.227)

Host is up (0.015s latency).

Not shown: 999 closed tcp ports (reset), 947 closed udp ports (port-unreach), 51 open|filtered udp ports (no-response)

PORT STATE SERVICE VERSION

6668/tcp open irc?

|\_irc-info: Unable to open connection

| fingerprint-strings:

| afp:

| MjB^Z

| .;H%

| MjB^Z

| .;H%

| MjB^Z

| giop:

| 4@nQ

|\_ ?vin%x

3702/udp open tcpwrapped

| wsdd-discover:

| Devices

| Message id: 10120738-7dd2-21b2-a205-4A1649881014

| Address: http://192.168.137.227:8000/onvif/device\_service

|\_ Type: n:NetworkVideoTransmitter tds:Device

3703/udp open tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port6668-TCP:V=7.92%I=7%D=4/13%Time=62572FA7%P=x86\_64-apple-darwin17.7.

SF:0%r(afp,27D,"\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0

SF:\0\xa0A\0\0\0\x01\xb8\xc3G\xdac\nS\xf5\xba\xbd2\x90\xb3\xf7R\rc\xdcK\xf

SF:3\x82rCg\xc0\x20\x0b\xb93\xcb\xa5\xcfM\|6\xb9U\xd0C\xbf\xfa\xeb:\r\x914

SF:\xd8\xdc\x1c\xfc\.\xcc\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0

SF:\x003\.3\0\0\0\0\0\0\xa0B\0\0\0\x01\xb8\xc3G\xdac\nS\xf5\xba\xbd2\x90\x

SF:b3\xf7R\rc\xdcK\xf3\x82rCg\xc0\x20\x0b\xb93\xcb\xa5\xcfM\|6\xb9U\xd0C\x

SF:bf\xfa\xeb:\r\x914\xd8\xdc\x9f\x95\xfe\x0f\0\0\xaaU\0\0U\xaa\0\0\0\0\0\

SF:0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\xa0C\0\0\0\x01\x08\x87\xcd\xa1

SF:\x9e\x83\r\xc3x\xf7a\x17>\xdeMjB\^Z\xfcQ\xa9\xc2s\x01t\xacBr{\x05\xf5\x

SF:ab\xb98\x92Yl\xfa\.6\xb7\.;H%\xda\xa9v\xa9\xea\xe5\0\0\xaaU\0\0U\xaa\0\

SF:0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\xa0D\0\0\0\x01\x08\x87

SF:\xcd\xa1\x9e\x83\r\xc3x\xf7a\x17>\xdeMjB\^Z\xfcQ\xa9\xc2s\x01t\xacBr{\x

SF:05\xf5\xab\xb98\x92Yl\xfa\.6\xb7\.;H%\xda\xa9\xd5\xd3\xfdc\0\0\xaaU\0\0

SF:U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\xa0E\0\0\0\x01

SF:\xb8\xc3G\xdac\nS\xf5\xba\xbd2\x90\xb3\xf7R\rc\xdcK\xf3\x82rCg\xc0\x20\

SF:x0b\xb93\xcb\xa5\xcf/\xef\x1dz\xbb\xcb\nH\xc8\x13\xa3\xaa\xc1<\xadj\xda

SF:\xef/D\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0

SF:\0\0\xa0F\0\0\0\x01\xb8\xc3G\xdac\nS\xf5\xba\xbd2\x90\xb3\xf7R\rc\xdcK\

SF:xf3\x82rCg\xc0\x20\x0b\xb93\xcb\xa5\xcf/\xef\x1dz\xbb\xcb\nH\xc8\x13\xa

SF:3\xaa\xc1<\xadjY\x86\xff\x87\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K

SF:\0\0\0\x003\.3\0\0\0\0\0\0\xa0H\0\0\0\x01\x08\x87\xcd\xa1\x9e\x83\r\xc3

SF:x\xf7a\x17>\xdeMjB\^Z\xfcQ\xa9\xc2s\x01t\xacBr{\x05\xf5\x12\xa2\xe5\x7f

SF:\xd4\.:\xef\x8d\xb3\x10\xd8\xbf3h`\x1b\x11E\x8f\0\0\xaaU")%r(giop,27D,"

SF:\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\xa0J\0\0\0

SF:\x01\x84J\x93#N\xef\xf97u5\xdaU\xab\xe9\xc2\xc3<e\xa2Y6\xaen\xd4\x84\xe

SF:2\xa2\x92\xc9\x92\xda\xa5\x9a&\xc5\r\xd4\xd5\xe2\xb2K\xe4\xb2I\xd3\x98Y

SF:\nz\x1c\x9a\x07\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.

SF:3\0\0\0\0\0\0\xa0K\0\0\0\x01\x08\x87\xcd\xa1\x9e\x83\r\xc3x\xf7a\x17>\x

SF:deMjk\xe1\]\x89\xa0\xeb\xf1\xe2\xfe\x99\xccI\x98P\x15\xf8\xcf\x07\xb7\x

SF:82}a%\x1c\x8a\x1dj\xd1\x92\xc4\)\xe8\x85!\xdc\xce\0\0\xaaU\0\0U\xaa\0\0

SF:\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\xa0L\0\0\0\x01\x08\x87\

SF:xcd\xa1\x9e\x83\r\xc3x\xf7a\x17>\xdeMjk\xe1\]\x89\xa0\xeb\xf1\xe2\xfe\x

SF:99\xccI\x98P\x15\xf8\xcf\x07\xb7\x82}a%\x1c\x8a\x1dj\xd1\x92\xc4\)\xe8&

SF:\[\xcbH\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\

SF:0\0\0\xa0N\0\0\0\x01\x84J\x93#N\xef\xf97u5\xdaU\xab\xe9\xc2\xc3<e\xa2Y6

SF:\xaen\xd4\x84\xe2\xa2\x92\xc9\x92\xda\xa5\xb9\x9a\xc9E\xc8\xf2V\x8b\xe5

SF:\xb2\x05Bb\x03\xd54@nQ\xa6\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0

SF:\0\0\x003\.3\0\0\0\0\0\0\xa0O\0\0\0\x01\x84J\x93#N\xef\xf97u5\xdaU\xab\

SF:xe9\xc2\xc3<e\xa2Y6\xaen\xd4\x84\xe2\xa2\x92\xc9\x92\xda\xa5\xb9\x9a\xc

SF:9E\xc8\xf2V\x8b\xe5\xb2\x05Bb\x03\xd54>\xb6\xe1\xe7\0\0\xaaU\0\0U\xaa\0

SF:\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\xa0P\0\0\0\x01\x08\x8

SF:7\xcd\xa1\x9e\x83\r\xc3x\xf7a\x17>\xdeMjk\xe1\]\x89\xa0\xeb\xf1\xe2\xfe

SF:\x99\xccI\x98P\x15\xf8\0\)\xb4f\xa0\xa8\xb4\x87\x20\xfaxm\x94\?vin%x\x1

SF:3\0\0\xaaU\0\0U\xaa\0\0\0\0\0\0\0\x08\0\0\0K\0\0\0\x003\.3\0\0\0\0\0\0\

SF:xa0Q\0\0\0\x01\x08\x87\xcd\xa1\x9e\x83\r\xc3x\xf7a\x17>\xdeMjk\xe1\]\x8

SF:9\xa0\xeb\xf1\xe2\xfe\x99\xccI\x98P\x15\xf8\0\)\xb4f\xa0\xa8\xb4\x87\x2

SF:0\xfaxm\x94\?vi\x10\xfd\xc8R\0\0\xaaU");

MAC Address: 84:7A:B6:23:C0:EA (AltoBeam (China))

Device type: general purpose

Running: Linux 2.6.X|3.X

OS CPE: cpe:/o:linux:linux\_kernel:2.6 cpe:/o:linux:linux\_kernel:3

OS details: Linux 2.6.32 - 3.10

Uptime guess: 0.020 days (since Wed Apr 13 12:50:19 2022)

Network Distance: 1 hop

TCP Sequence Prediction: Difficulty=263 (Good luck!)

IP ID Sequence Generation: All zeros

TRACEROUTE

HOP RTT ADDRESS

1 15.45 ms 101207387.mshome.net (192.168.137.227)

NSE: Script Post-scanning.

Initiating NSE at 13:18

Completed NSE at 13:18, 0.00s elapsed

Initiating NSE at 13:18

Completed NSE at 13:18, 0.00s elapsed

Initiating NSE at 13:18

Completed NSE at 13:18, 0.00s elapsed

Read data files from: /usr/local/bin/../share/nmap

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 1280.82 seconds

Raw packets sent: 2779 (128.914KB) | Rcvd: 2086 (139.550KB)

We attempted to connect to an open TCP port on :6668, but a netcat connection did not provide any prompts.

**Wireshark**

We did a complete packet capture of network traffic during our testing, which can be found at:

<https://drive.google.com/file/d/1E_87v9dGABbrcbCqVoNnNYySncdzL88p/view?usp=sharing>

We have been analyzing this trace as well, with a few key takeaways:

* Camera is controlled by an encrypted MQTT connection to an AWS server
* No data is transmitted to the camera locally

**Nessus Vulnerability Scanner**



#### **OS Identification**

Remote operating system : Linux Kernel 2.6

Confidence level : 56

Method : MLSinFP

#### **Nessus SYN scanner**

Port 6668/tcp was found to be open

#### **Open Network Video Interface Forum (ONVIF) Protocol Detection**

The ONVIF service listening on UDP port 3702 advertises

the following information:

Endpoint: http://192.168.137.227:8000/onvif/device\_service

Name: IPC\_101207387