IoT devices

Maryam Gadiali – 30/07/2024

IoT device

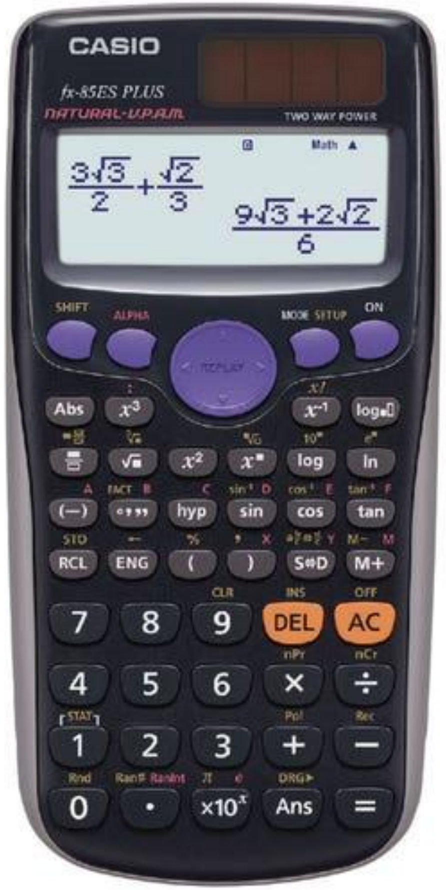
A device with software and sensors that can receive and transmit data over the internet.

Home use

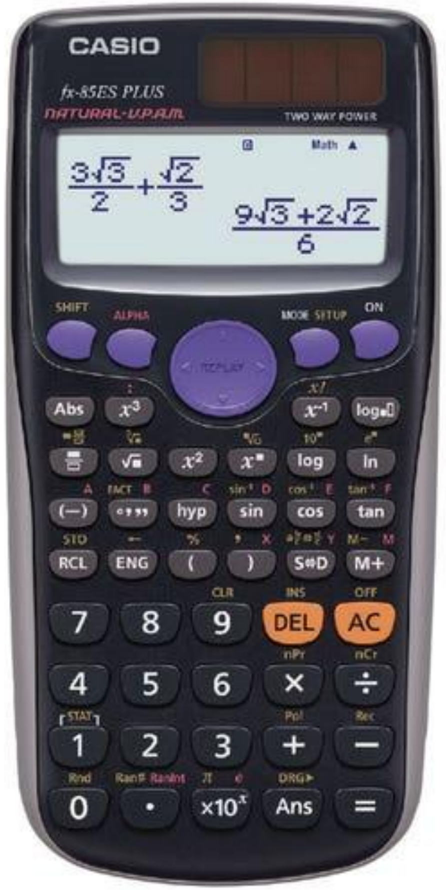
“Smart” or online

kg
min
Defrost
Defrost
Defrost
Timer
Time
Stop
Start

Not an IoT device


CASIO
fx-85ES PLUS
NATURAL-V.P.A.M.
TWO WAY POWER

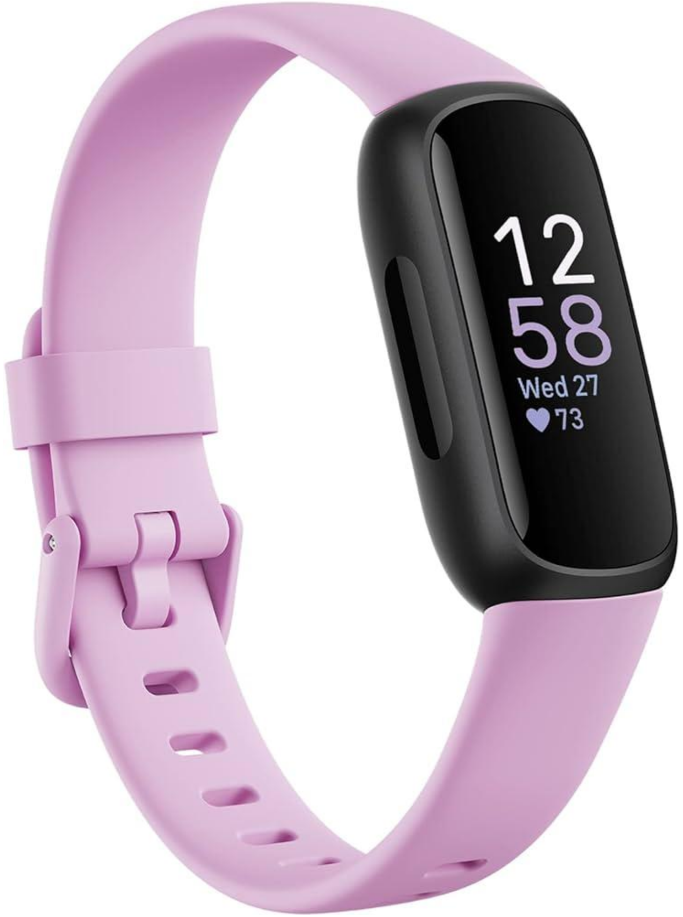
Not an IoT device



Not an IoT device

12
58
Wed 27
♥73

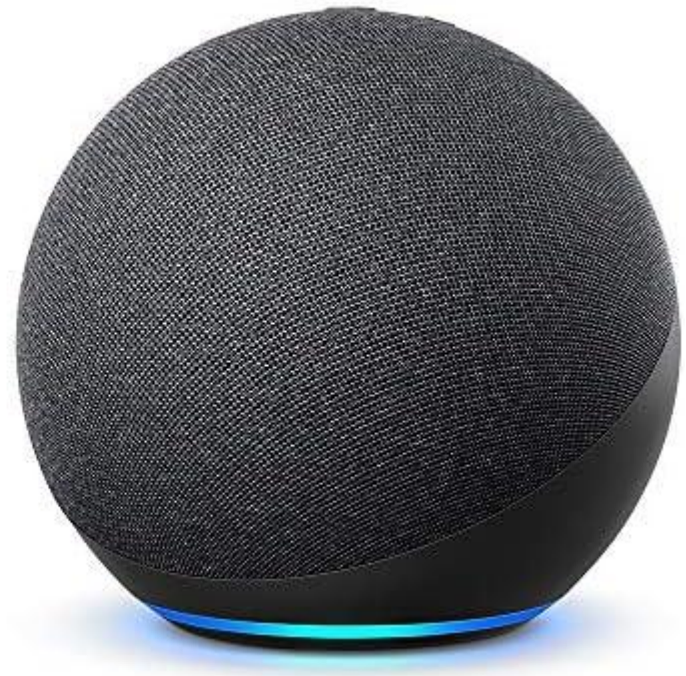
Is an IoT device



8:59
VIDAA
It's all about U
Press to Manage Apps
NETFLIX
YouTube
prime video
Disney+
deezer
plex
CANAL+
VOYO
tv
LEPŠÍ.TV
Televize Seznam
EVROPA2
Kidoodle.TV
VIDAA tv+
Top Picks
HOME
DEFENDING JACOB
HOME BEFORE DARK
SENCOR

Is an IoT device

Is an IoT device



Also IoT devices...

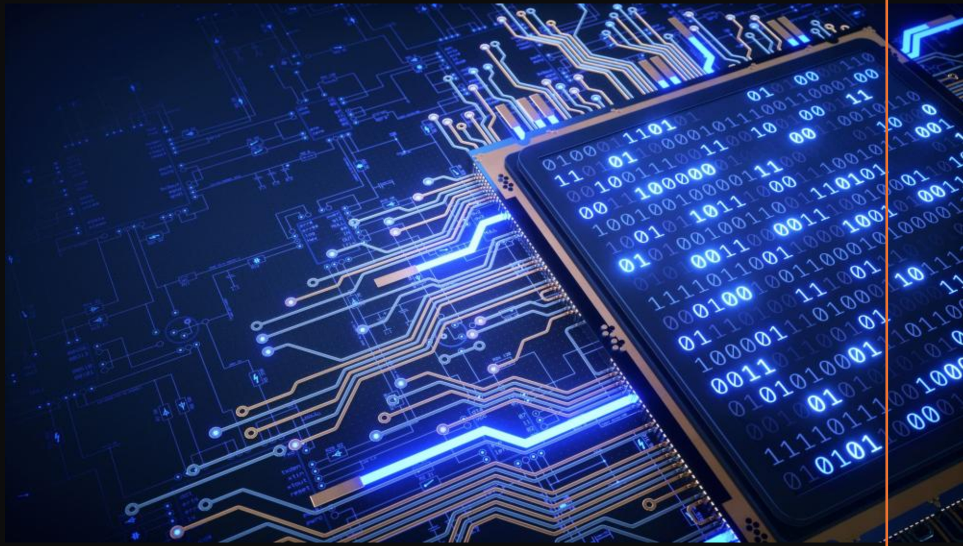
Stats

- 77 percent of UK adults own at least one smart home device
- By 2050 there will be 24 billion interconnected devices worldwide

- https://publications.parliament.uk/pa/cm5803/cmselect/cmcumeds/157/report.html

Problems with available IoT devices

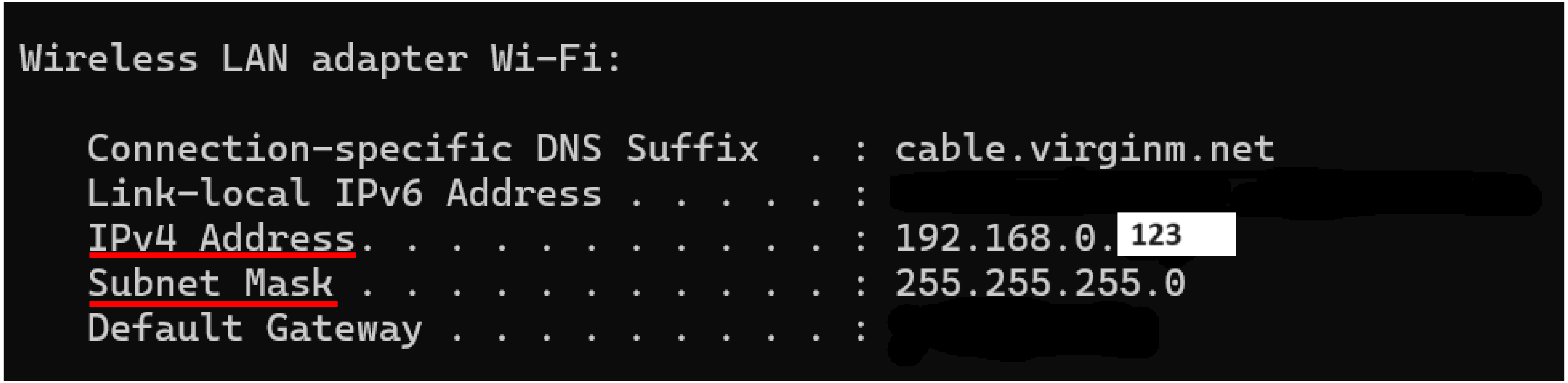
- 57 percent of connected devices are vulnerable to medium- to high-severity attacks
- Convenience and price over security
- Lack of encryption (HTTP instead of HTTPS)
- Port forwarding issues
- Default login
- Not updating to the latest version



IoT cameras

1. Finding out home wifi details

ipconfig



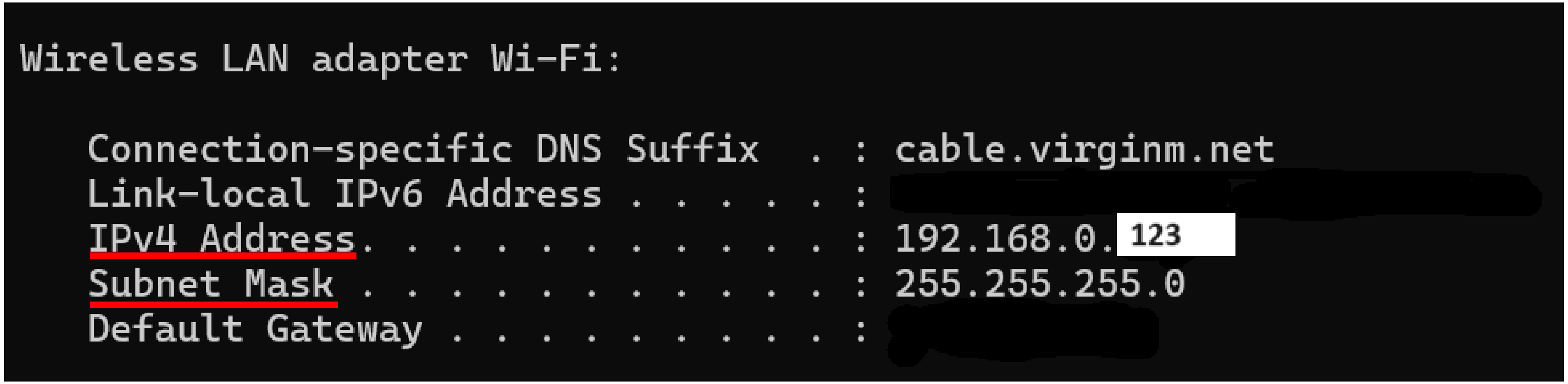
```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : cable.virginm.net
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 192.168.0.123
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : [redacted]
```

2. Running nmap

- Port scanning tool
- -A scan
- nmap –A <Target>

Open
Closed
Filtered, Blocked
Port scanning response types



```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : cable.virginm.net
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 192.168.0.123
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : [redacted]
```

IPv4 Addr = 192.168.0.123

Subnet mask = 255.255.255.0

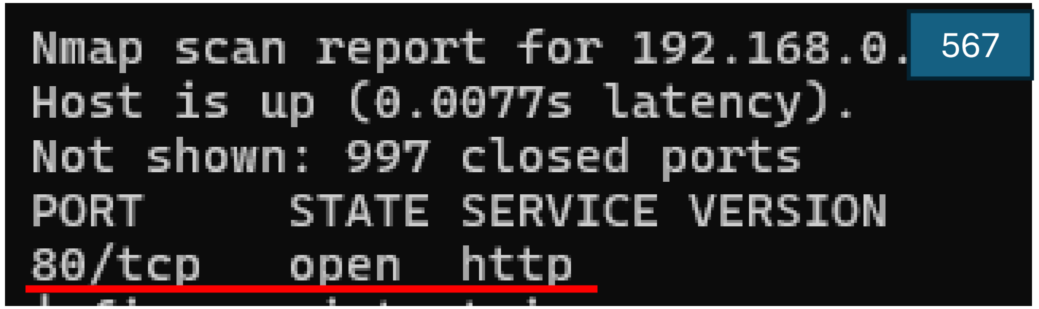
CIDR notation = 192.168.0.123/24

24 bits (Network) + 8 bits (Host) = 32 bits (IPv4)

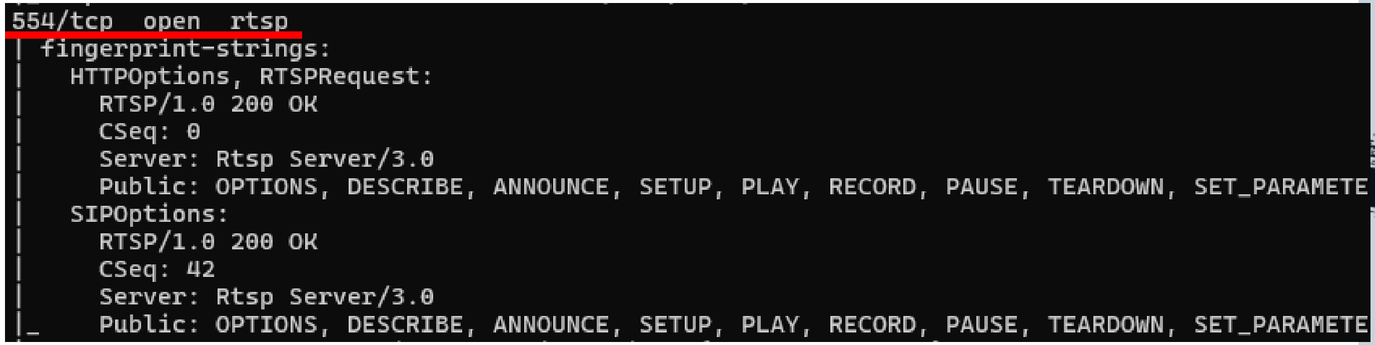
nmap –A 192.168.0.123/24

3. Analysing the nmap output

- Port 554 (RTSP) along with port 80 (HTTP) (or 443 – HTTPS)
- RTSP methods – OPTIONS, PLAY, RECORD, PAUSE…
- Note down attached ip address

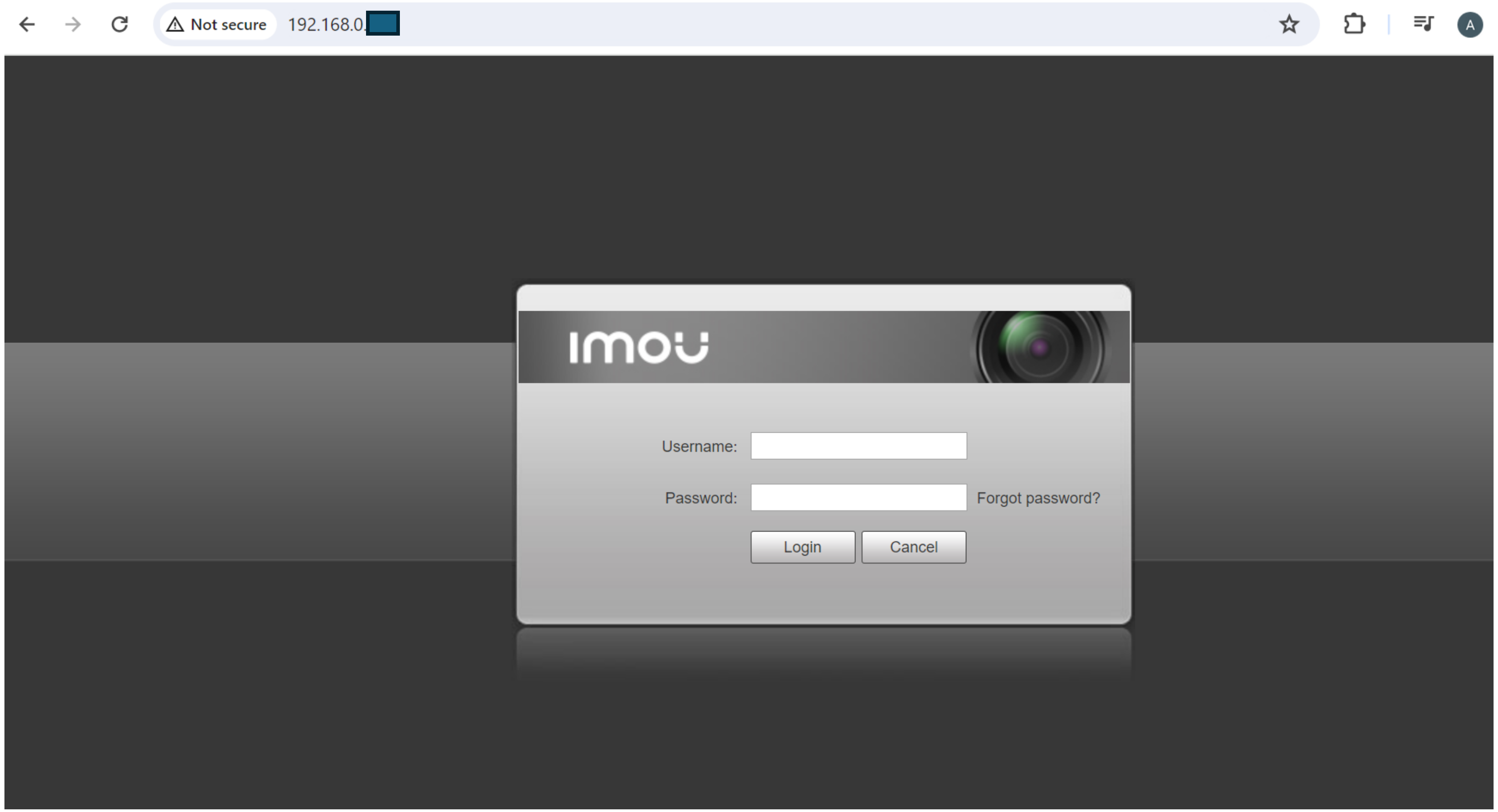


```
Nmap scan report for 192.168.0.567
Host is up (0.0077s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http
```



```
554/tcp  open  rtsp
| fingerprint-strings:
|   HTTPOptions, RTSPRequest:
|     RTSP/1.0 200 OK
|     CSeq: 0
|     Server: Rtsp Server/3.0
|     Public: OPTIONS, DESCRIBE, ANNOUNCE, SETUP, PLAY, RECORD, PAUSE, TEARDOWN, SET_PARAMETE
|   SIPOptions:
|     RTSP/1.0 200 OK
|     CSeq: 42
|     Server: Rtsp Server/3.0
|_    Public: OPTIONS, DESCRIBE, ANNOUNCE, SETUP, PLAY, RECORD, PAUSE, TEARDOWN, SET_PARAMETE
```

4. Gaining access to the camera



192.168.0.[redacted]

Next steps

- Default username and passwords
- Wireshark Packet capturing (HTTP) for authentication details
- CVE lists for known vulnerabilities

Mitigations

- Change the default username and password
- Use strong details
- Disable Http use if possible
- Regularly update
- Disable port forwarding
- Disable UPnP (Universal Plug and Play)
- Network segmentation

Thank you for listening

Maryam Gadiali