VR Model P1 - 360 degree camera

May 19, 2020

This article is one of my very old assessment for fun i did (and it is done 2017) got it by recovering hard disk and assigned **CVE ID - (CVE-2020-23512).**

Here my target to test 360 degree camera which trending in the IP camera world recently, what we going test model P1 VR camera.

What is VR camera..?
In photography, an omnidirectional camera (from "Omni", meaning all) is a camera with a 360-degree field of view in the horizontal plane, or with a visual field that covers (approximately) the entire sphere. Omnidirectional cameras are important in areas where large visual field coverage is needed, such as in panoramic photography and robotics.

VR CAM P1 Proxy Eye Fisheye Camera IP 3D Vr 360 Degree Panoramic 960P Wi-Fi CCTV Camera With Sd Memory Card Slot Multi Viewing Mode

Features of this VR CAMERA:

Brand	VR CAM
Model	P1
Product Dimension	15 x 15 x 5 cm
Resolution	960p
Android/iOS Devices	Additional Features
Additional features	* 360 Degree Panorama + 3D VR + WIFI & Wired RJ45 + TF Card Slot + Two Way Audio *Multi Angle Monitor: Mode 1: Electronic PTZ, Mode 2:Panoramic, Mode 3: Corridor, Mode 4:Tranditional Split Screen, *1/3 Inch CMOS Sensor, Resolution: 1536 x 1536, Lens 1.19mm Visual Angle 360 degree, 3MP HD *One Camera = 4 to 6 piece common camera
Optical Zoom	16 X
Connector Type	Wireless ,Wired
Material	Plastic
Lens Type	Fisheye
Voltage	12 Volts
Wattage	130

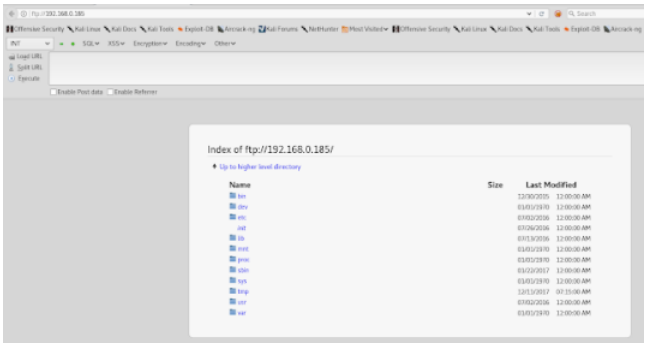
For config the Device follow the document :
http://www.global-export-import.eu/WEBSET_DOWNLOADS/611/AN-H360-1_EN.pdf

Lets start the assessment:
As part of the security assessment i just connected Ethernet to device and it is assigned IP

started scanning the IP address of the device and got the results as shown below

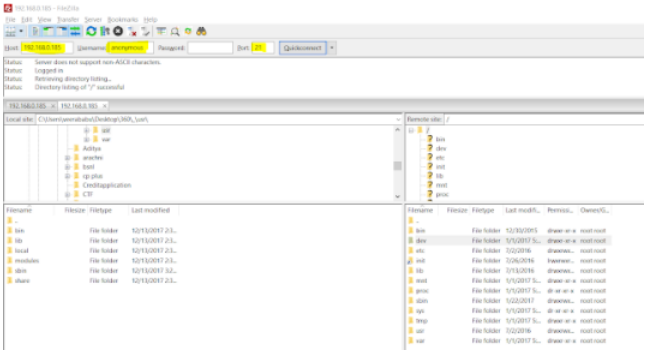
```
root@kali:~# nmap -sC 192.168.0.185

Starting Nmap 7.60 ( https://nmap.org ) at 2017-12-11 02:34 EST
Nmap scan report for 192.168.0.185
Host is up (0.12s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| total 0
| drwxr-xr-x    2 root     root          1029 Dec 30  2015 bin
| drwxr-xr-x    5 root     root             0 Jan  1  1970 dev
| drwxrwxrwx    5 root     root           283 Jul  2  2016 etc [NSE: writeable]
| lrwxrwxrwx    1 root     root            11 Jul 26  2016 init -> bin/busybox
| drwxrwxrwx    3 root     root           705 Jul 13  2016 lib [NSE: writeable]
| drwxr-xr-x    2 root     root             0 Jan  1  1970 mnt
| dr-xr-xr-x   56 root     root             0 Jan  1  1970 proc
| drwxrwxrwx    2 root     root           763 Jan 22  2017 sbin [NSE: writeable]
| dr-xr-xr-x   13 root     root             0 Jan  1  1970 sys
| drwxr-xr-x    2 root     root             0 Dec 11 07:15 tmp
| drwxrwxrwx    8 root     root           102 Jul  2  2016 usr [NSE: writeable]
| drwxr-xr-x    6 root     root             0 Jan  1  1970 var
|_ftp-bounce: bounce working!
| ftp-syst:
|   STAT:
| Server status:
|  TYPE: BINARY
| Ok
23/tcp   open  telnet
80/tcp   open  http
|_http-title: Site doesn't have a title (text/html).
6789/tcp open  ibm-db2-admin
MAC Address: 9C:A3:A9:1B:13:71 (Guangzhou Juan Optical and Electronical Tech Joint Stock)
```

That's interesting some ports are open like 21,23,6789 with details and it is port number 21 ftp-anon is possible means anonymous credentials will work and if there is no "auth" direct will get
- lets see

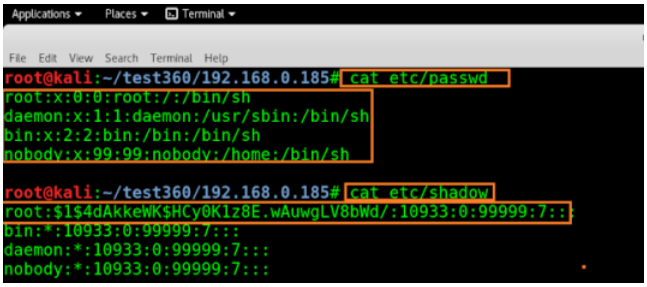


There is no authentication on the FTP and it is giving the direct access to the filesystem of camera.We already got the firmware access from port number 21 (FTP) will check through web interface or we can download firmware from the FTP location using WGET (wget -r) or use FTP Client download filezilla)

FTP client File-zilla Access

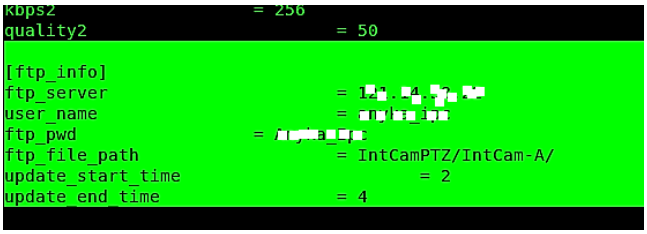


Filesystem analysis is always main part of the IoT Devices Pentesting , After downloading firmware just dig deep all files to get confidential information.In etc/password and etc/shadow having the hardcoded information's

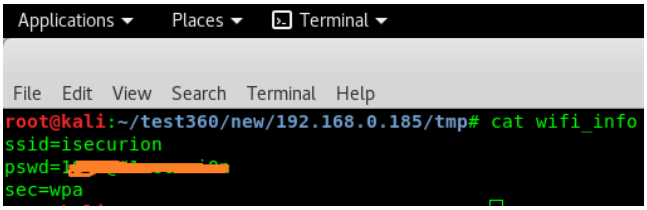


MD5 Hashed

And JFFS filesystem files consisting
Remote FTP Server IP information with credentials

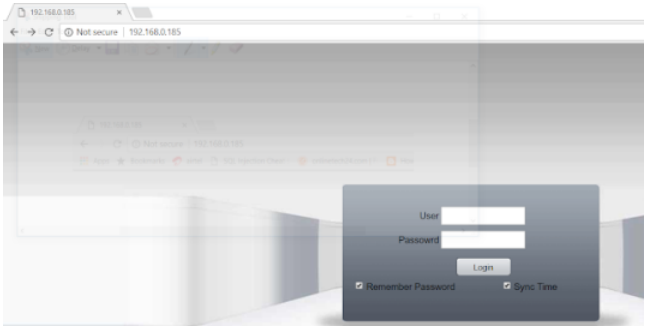


Digging around some more i found some treasure in the form of the router's (yes the work network) Wi-Fi password in plaintext at /tmp/wifi_info.



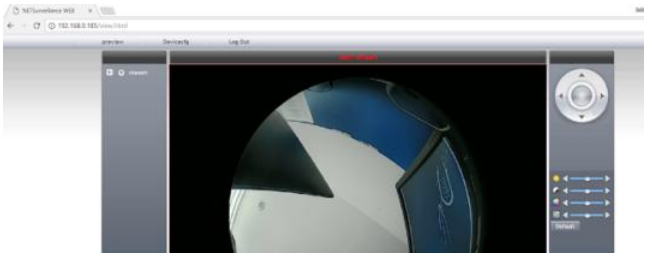
When we checking the web interface of device, and we got to know the login page having the business logic vulnerability,

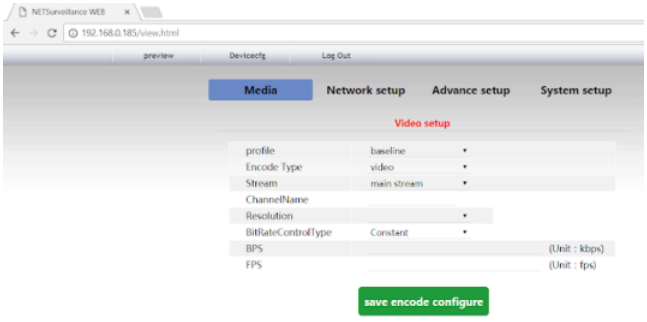
That is without credentials we can get access of admin control panel, below image shows the login page



There are some parameters from embedded application it was observed that the application is possible to access the direct admin control panel without credentials

http://192.168.0.185/view.html





To leave a comment, click the button below to sign in with Google.

Popular posts from this blog

Dumping the Firmware from the device Using buspirate - SPI

June 05, 2019

One of the best way to get the firmware from the hardware While doing penetration testing there are scenarios in which we need to dump the firmware from the devices.This method is typically used when there are no firmware's available from

READ MORE

Buspirate v3.6 firmware upgrade from USB

June 19, 2021

Buspirate: The Bus Pirate v3.6a, created by Ian Lesnet, is a troubleshooting tool that communicates between a PC and any embedded device over 1-wire, 2-wire, 3-wire, UART, I2C, SPI, and HD44780 LCD protocols - all at voltages from 0-5.5VDC. …

READ MORE

Mr-IoT

Report Abuse

MR-IOT

VISIT PROFILE

Blog Posts

Labels

Followers (0)

Total Pageviews

63784