Vulnerability of CCTV & IP Camera

HYUNWOO KIM & HAENG-UN HA & MINJOON PARK

NSHC Pte, Ltd.

Your Partner for Cyber defense & Intelligence
Introduce

- Hyunwoo KIM  • Work NSHC in Singapore
- Haeng-un HA  • Work NSHC in Korea
- Minjoon PARK  • Worked NSHC in Singapore
Contents

- Abstract
- How to hack
- Vulnerability
- Backdoor
- Scenario and DEMO
- Conclusion
Abstract

- IP Camera (IP-CAM, Network Camera)
  - An Internet protocol camera, or IP camera, is a type of digital video camera commonly employed for surveillance (Wikipedia)
Abstract

- IoT Device is increasingly affordable
Abstract

- IP Camera are used from various areas
  - Home / Company / Public Place
  - Government / Organization
  - and so on...
How to hack IP-CAM

Buy → Install → Extract → Analysis → Exploit
How to hack IP-CAM | BUY products

In Singapore
- Go to Challenger
  ✓ There are many IoT devices
- Choice the goods
  ✓ D* / T* / L* vendor

In Korea
- Internet Shopping
  ✓ Used market

<table>
<thead>
<tr>
<th>사용상품</th>
<th>신상품</th>
<th>현재가</th>
<th>구매가</th>
</tr>
</thead>
<tbody>
<tr>
<td>네트워크 클라우드/WiFi/안드로이드 호환 경보/수신 모듈/TF카드 - 내장모듈 - 제조기업: Matomo 기업</td>
<td>30,000원</td>
<td>180,000원</td>
<td></td>
</tr>
<tr>
<td>심장대기/마이크로소프트 라이브러리 VX-3 000원 PC화상카메라/4메트릭/2장</td>
<td>5,000원</td>
<td>24,000원</td>
<td></td>
</tr>
<tr>
<td>PC집</td>
<td>15,500원</td>
<td>25,000원</td>
<td></td>
</tr>
</tbody>
</table>
How to hack IP-CAM | INSTALL product

- Install IP-CAM
How to hack IP-CAM | EXTRACT Firmware

● How to get Firmware
  ✓ Download firmware from Vendor’s official Homepage
  ✓ If we can get root shell, try partition dump
  ✓ Use the hardware (ex: UART, JTAG)
  ✓ Flash memory dump
  ✓ Network packet dump

● Tools
  ✓ Firmware Modification Kit
  ✓ Binwalk
How to hack IP-CAM | Analysis & Exploit

- Extracted files analysis

```
loc_435E8:
la    $a0, 0x4D0000
nop
addiu $a0, (aVarRunIpcamera - 0x4D0000)  # "/var/run/ipcamera.pid"
la    $t9, 0x430000
nop
addiu $t9, (loc_435C00 - 0x430000)
nop
jalr  $t9 ; loc_435C00
nop
lu    $gp, 0x40+var_38($fp)
bgez  $v0, loc_435FA4
nop
```
How to hack IP-CAM | Analysis & Exploit

- Web Hacking

![Image of Wireless IP Camera Status](image)
Vulnerability

- Vulnerability summary
  - ✓ XSS(Cross Site Scripting)
  - ✓ Information Disclosure
  - ✓ Buffer OverFlow
  - ✓ Protocol Vulnerability
  - ✓ File Download
  - ✓ Policy Fail
  - ✓ and so on...
Vulnerability

- XSS (Cross Site Scripting)
Vulnerability

- Information Disclosure

```
Hostname=
description=<script>alert('NSHC');</script>
defname=
mac=00:14:bf:71:1c:09
resolution=320
type=mpeg4
voice_in=off
voice_out=on
pt=on
resolutions=704*480,640*480,320*240,160*120
```
Vulnerability

- Buffer OverFlow

File index.htm not found
Vulnerability

- Buffer OverFlow

```c
int __fastcall psk_bof_hub_B0CC(int a1)
{
    char v2; // [sp+0h] [bp-164h]05
    int v3; // [sp+4h] [bp-168h]86
    int v4; // [sp+8h] [bp-170h]85
    char *v5; // [sp+14h] [bp-178h]85
    int v6; // [sp+18h] [bp-180h]01
    int v7; // [sp+1Ch] [bp-184h]01

    v7 = a1;
    sub_83E4("Generate_WpaPSKhn");
    v6 = find_val(v7, "next_file");
    if (!v6)
        v6 = find_val(v7, "this_file");
    if (!v6)
        v6 = dword_39EC8;
    i4 = (char *)find_val(v7, "psk");
    v4 = WLANReadConfigData(&v2);
    if (!i4)
        strcpy((char *)&i3, i4);
    v4 = WLANGenerateWPAKeys(&v2);
    v4 = WLANWriteConfigData(v2);
    sub_83E4("WPA_PSK save to configWh");
    return 0;
}
```
Vulnerability

- File Download
Vulnerability

- Policy Fail
  - ✔ Password brute-force attack is allowed
  - ✔ Any fail2ban?

  ✔ Mobile app provides network scan for cam with default password
  ✔ No auth process
중국산 CCTV에서 백도어가 발견됐다

The backdoor was discovered in China CCTV.
Backdoor

- We classified backdoors into two categories
  - Unintended Backdoor
    » Utilized for device management
    » Utilized to access the device
  - Intended Backdoor
    » Surveillance and other arbitrary purpose
    » Utilization for industry spy
    » Encapsulating the existence of the backdoor using encryption
Backdoor

- We found some backdoors in IP-CAM
  - ✔ Unintended Backdoor – “D* vendor”
  - ✔ Intended Backdoor – “T* vendor”
  - ✔ Unclassified – “L* vendor”

- We choose a product for each company, and We succeeded to find it for all of them :(
## Backdoor

- Disclosure of IP-CAM Administrator ID / PW

### Camera Information

- **Camera Name:** [redacted]
- **Model:** [redacted]
- **IP Address:** 192.168.1.121
- **MAC Address:** c4:6e:1e:a8:11:7d

### Camera Login Information

- **Camera Login Username:** admin
- **Camera Login Password:** admin
- **Show password:** [on]

Please click the below button to remove your [redacted] from your account:

**Delete Camera**

**Save**
Backdoor

- Web based Backdoor
Backdoor

- Telnet based Backdoor

Open Telnet/FTP (inetd) Daemon successfully!
Scenario and DEMO

- Crack the D* Vendor Password

1. Malicious program is with CAM on same network (not necessary but recommended)
2. Send some packets to CAM
3. Get md5sum of PASSWORD from response
4. CRACK IT
Conclusion

- IPCAM has many vulnerability!!

- Also, IPCAM has backdoor