

# Cable Haunt - How to hack a 100 million devices

## Driving IT 2020

Lyrebirds ApS

5. marts, 2020

#whoami

**Jens Hegner Stærmose**

Partner in Lyrebirds

We discovered Cable Haunt



# Agenda

- ▶ TLDR
- ▶ How we discovered Cable Haunt
- ▶ Disclosure process
- ▶ Key takeaways

# Cable Haunt - What is it?



\*  $\times 00.000.000$

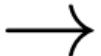
```
~] ssh root@51.91.98.143
root@51.91.98.143's password:
Last login: Mon Feb 17 14:49:29 2020 from 5.179.90.150
[root@vps730674 ~]# sudo rm -rf /
```

- ▶ A vulnerability in cable modems (COAX)
- ▶ Affects hundreds of millions of devices
- ▶ Complete control through client with LAN access
- ▶ Browser, E-mail client, IP-camera etc.

## Cable Haunt - What can it do?



Denial of Service



Persistent Network  
Control

# Cable Haunt - How does it work?

- ▶ Stack buffer overflow in Spectrum Analyzer
  - ▶ Diagnostic tool on LAN-endpoint
- ▶ Unprotected websocket
  - ▶ No verification of Origin or Host
  - ▶ Default passwords
- ▶ Javascript in browser compromises modem

# How did we discover Cable Haunt

## How did we discover Cable Haunt



### No internet

Try:

- Checking the network cables, modem, and router
- Reconnecting to Wi-Fi

ERR\_INTERNET\_DISCONNECTED

# How did we discover Cable Haunt

- ▶ Started poking around the administrator panel
- ▶ Unknown device

The screenshot shows a web-based administration interface for a Technicolor router. The top navigation bar includes links for Gateway, VoIP, Administration, Status, Network (which is selected), Advanced, Firewall, Parental Control, Wireless, USB, and Logout. On the left, a sidebar lists options like LAN, WAN, Computers, DDNS, Time, FTP Diagnostics, Portbase, and Passthrough. The main content area is titled 'Network' and specifically 'Computers'. It displays information about DHCP clients, including their MAC addresses, IP addresses, subnet masks, and duration. Two clients are listed:

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
9cb6d0d35c37	192.168.000.010	255.255.255.000	D:07 H:00 M:00 S:00	--- --- --- ---	<input type="radio"/>
e0885d89c2a7	192.168.000.011	255.255.255.000	D:07 H:00 M:00 S:00	--- --- --- ---	<input type="radio"/>

Below the table, the current system time is shown as 'Current System Time : --- --- --- ---'. A 'Force Available' button is located at the bottom right of this section.

# How did we discover Cable Haunt

- ▶ Started poking around the administrator panel
- ▶ Unknown device

The screenshot shows a web-based administration interface for a Technicolor router. The top navigation bar includes links for 'Gateway', 'VoIP', 'Logout', and tabs for 'Status', 'Network', 'Advanced', 'Firewall', 'Parental Control', 'Wireless', and 'USB'. The 'Network' tab is selected. On the left, a sidebar lists 'LAN', 'WAN', 'Computers', 'DDNS', 'Time', 'FTP Diagnostics', 'Portbase', and 'Passthrough'. The main content area is titled 'Network' and contains a section for 'Computers'. It states: 'Computers : This page shows the status of the DHCP clients and current system time.' Below this is a table titled 'DHCP Clients' with columns: MAC Address, IP Address, Subnet Mask, Duration, Expires, and Select. Two rows of data are shown:

MAC Address	IP Address	Subnet Mask	Duration	Expires	Select
9cb6d0d35c37	192.168.000.010	255.255.255.000	D:07 H:00 M:00 S:00	-----	<input checked="" type="radio"/>
e0885d89c2a7	192.168.000.011	255.255.255.000	D:07 H:00 M:00 S:00	-----	<input type="radio"/>

Below the table, the 'Current System Time' is listed as '---- - - - - : - - - -'. A 'Force Available' button is located at the bottom right of this section.

# How did we discover Cable Haunt

- ▶ Port scan device
- ▶ Telnet (application protocol)
- ▶ Root user... Password?

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-02 17:02 CET
Nmap scan report for localhost (127.168.0.11)
Host is up (0.000096s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE
23/tcp    open  telnet
53/tcp    open  domain
46807/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.44 seconds
→ ~
```

# How did we discover Cable Haunt

Password: "**broadcom**"

## How did we discover Cable Haunt

- ▶ No external access
- ▶ Administrator panel allows port forward
- ▶ Webserver accepts foreign domain names
- ▶ DNS rebind
- ▶ But they still have unique credentials!
- ▶ ... we thought

## How did we discover Cable Haunt

Password: "**aDm1n\$TR8r**"

## Contacting ISP

- ▶ ISP acknowledges issue
  - ▶ "But, you won't get into the eCos..."

# Contacting ISP

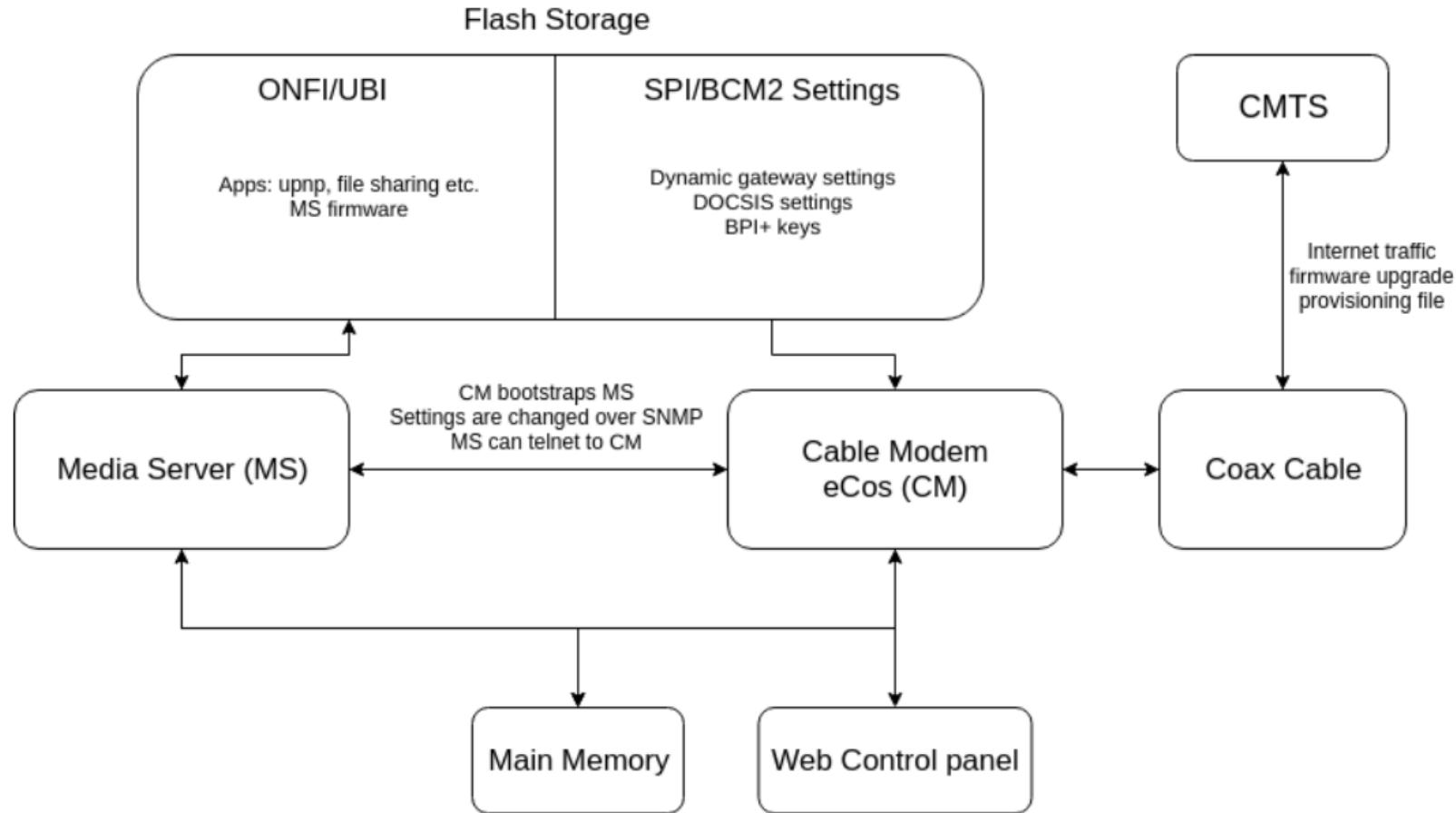
- ▶ ISP acknowledges issue
  - ▶ "But, you won't get into the eCos..."
- ▶ What is eCos, DOCSIS??
- ▶ We have no
  - ▶ documentation
  - ▶ datasheets
  - ▶ firmware
  - ▶ industry knowledge
  - ▶ ...

# Contacting ISP

- ▶ ISP acknowledges issue
  - ▶ "But, you won't get into the eCos..."
- ▶ What is eCos, DOCSIS??
- ▶ We have no
  - ▶ documentation
  - ▶ datasheets
  - ▶ firmware
  - ▶ industry knowledge
  - ▶ ... even the right screwdriver



# Architecture of TC7230



# From nothing to binary blob

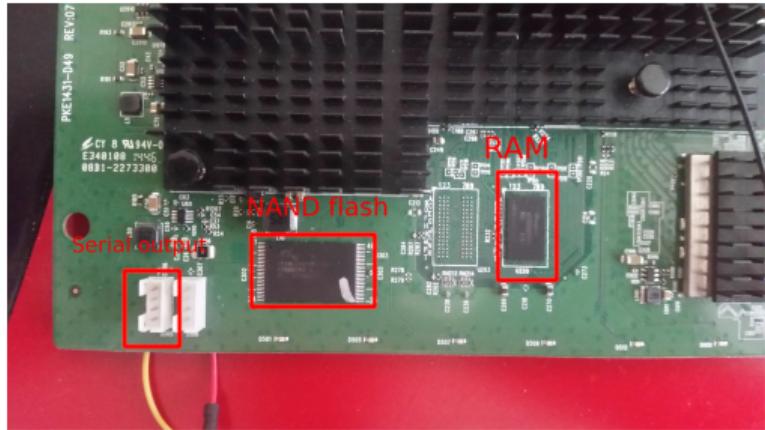
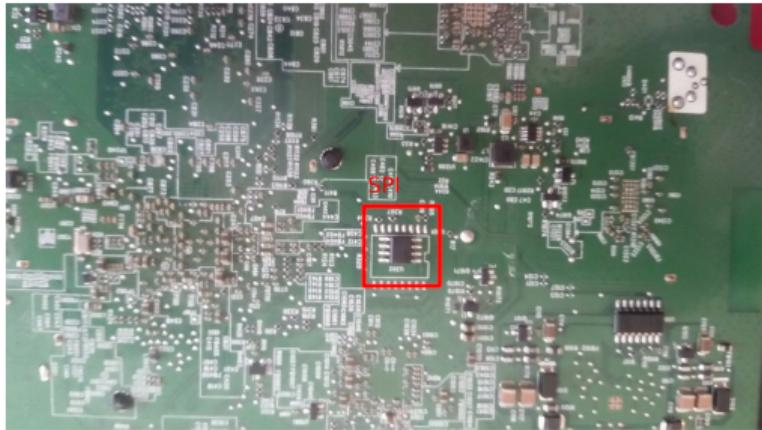


Figure 1: Front and back side of board

## From nothing to binary blob

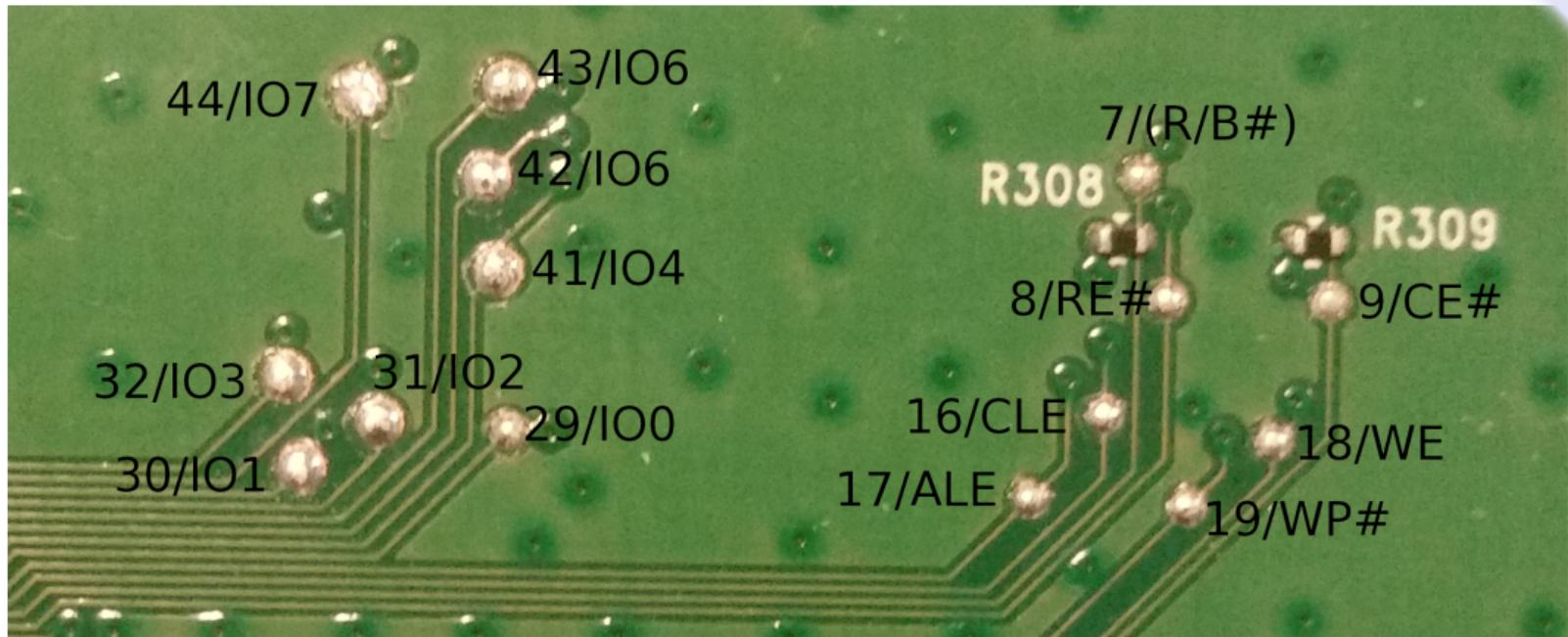


Figure 2: Soldering points for NAND flash

# From binary blob to overflow

```
+ tcfirmware TC7230-EB.01.25-160301-F-5FF.bin
```

# From binary blob to overflow

```
→ tcfirmware binwalk TC7230-EB.01.25-160301-F-5FF.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
---------	-------------	-------------

```
→ tcfirmware ↵
```

# From binary blob to overflow

```
→ tcfirmware binwalk TC7230-EB.01.25-160301-F-5FF.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
-----
→ tcfirmware binwalk -I TC7230-EB.01.25-160301-F-5FF.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
-----
51          0x33      LZMA compressed data, properties: 0x6E, dictionary size: 0 bytes, uncompressed size: 0 bytes
92          0x5C      LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 28
98643604054482944 bytes
3758         0xEAЕ      PC bitmap,
12174         0x2F8E     Private key in DER format (PKCS header length: 4, sequence length: -21193
12174         0x2F8E     Certificate in DER format (x509 v3), header length: 4, sequence length: -21193
17388         0x43EC     BFF volume entry, AIXv3, file size: 2128155235, compressed size: -332173556, file name: "ÿ» r
íç]`{%i<U0
xnåæþ`ð
"
18424         0x47F8      Linux EXT filesystem, blocks count: 1552464976, image size: 1589724135424, invalid state invalid error behavior invalid major revision rev -1390415010.-21217, ext4 filesystem data, UUID=3f01df5b-078e-2734-5d9b-157b75
f675f6, volume name "â=§ÜÜ[  `ð"
→ tcfirmware [
```

# From binary blob to overflow

```
→ tcfirmware binwalk TC7230-EB.01.25-160301-F-5FF.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
-----
→ tcfirmware binwalk -I TC7230-EB.01.25-160301-F-5FF.bin

DECIMAL      HEXADECIMAL      DESCRIPTION
-----
51          0x33      LZMA compressed data, properties: 0x6E, dictionary size: 0 bytes, uncompressed size: 0 bytes
92          0x5C      LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 28
98643604054482944 bytes
3758         0xEAE     PC bitmap,
12174         0x2F8E    Private key in DER format (PKCS header length: 4, sequence length: -21193
12174         0x2F8E    Certificate in DER format (x509 v3), header length: 4, sequence length: -21193
17388        0x43EC    BFF volume entry, AIXv3, file size: 2128155235, compressed size: -332173556, file name: "ÿ» r
íç]`{%i<U0
xnåæþ`ð
"
18424         0x47F8    Linux EXT filesystem, blocks count: 1552464976, image size: 1589724135424, invalid state invalid error behavior invalid major revision rev -1390415010.-21217, ext4 filesystem data, UUID=3f01df5b-078e-2734-5d9b-157b75
f675f6, volume name "â=§ÜÜ[`¶`ð"

→ tcfirmware
```

# From binary blob to overflow

```
02c00000: a82d 0005 0100 01ff 55f7 eeee 0050 33a8 |.-.....U....P3.|  
02c00010: 8000 4000 5443 3732 3330 2e53 2d45 422e |..@.TC7230.S-EB.|  
02c00020: 3437 2e30 342d 3135 3039 3135 2d46 2d35 |47.04-150915-F-5|  
02c00030: 4646 2e62 696e 0000 0000 0000 0000 0000 |FF.bin.....|  
02c00040: 0000 0000 0000 0000 0000 0000 0000 0000 |.....|  
02c00050: 0000 0000 b2aa 0000 359f 0dbd 5d00 0010 |.....5...]...|
```

```
Signature: a82d  
Control: 0005  
Major Rev: 0100  
Minor Rev: 02ff  
Build Time: 2016/3/2 10:16:39 Z  
File Length: 5267860 bytes  
Load Address: 80004000  
Filename: TC7230-EB.01.25-160301-F-5FF.bin  
HCS: 3b20  
CRC: 34267371
```

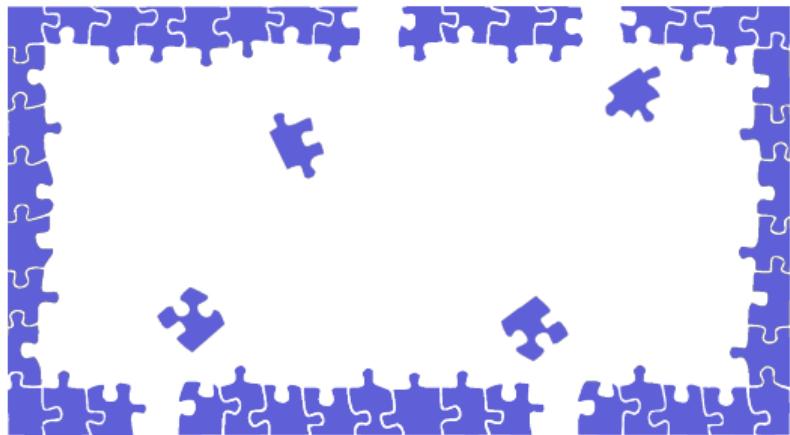
```
Performing CRC on Image...  
Detected LZMA compressed image... decompressing...
```

```
Decompressed length unknown. Padded to 100663296 bytes.
```

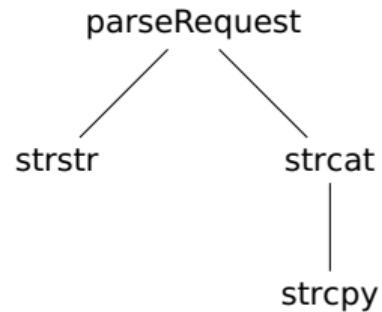
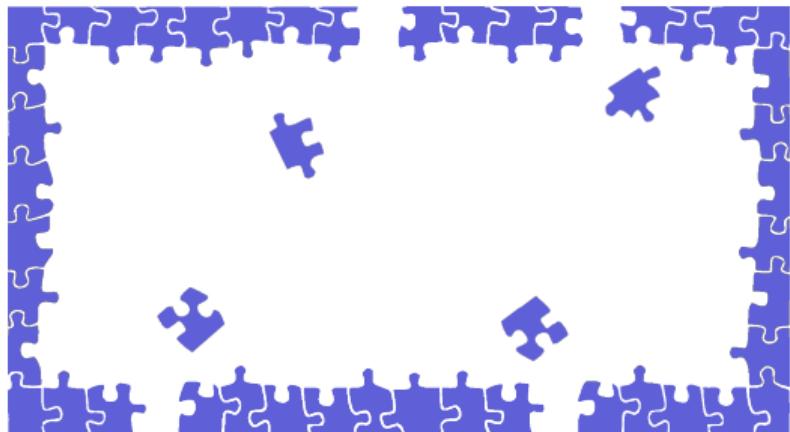
# Reverse Engineering

Password: "**private**"

# Reverse Engineering



# Reverse Engineering



# Analysis Tool

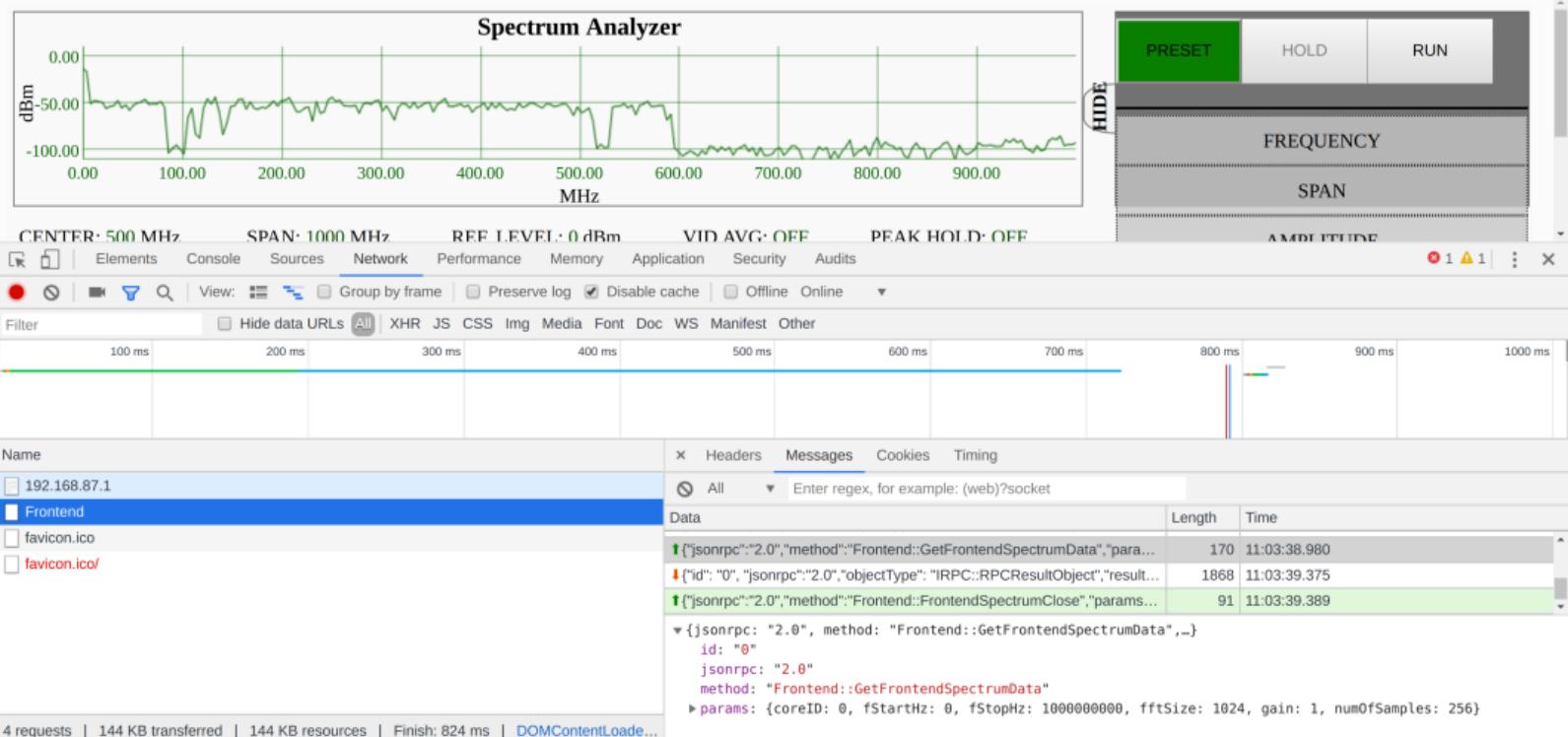


Figure 3: spectrum analyzer

## Sample JSON Request

```
1  {
2      id: 0,
3      jsonrpc: "2.0",
4      method: "Frontend::GetFrontendSpectrumData",
5      params: {
6          coreID: 0,
7          fStartHz: 0,
8          fStopHz: 1000,
9          fftSize: 1024,
10         gain: 1,
11         num0fSamples: 256
12     }
13 }
```

## Sample JSON Request

```
1  {
2      id: 0,
3      jsonrpc: "2.0",
4      method: "Frontend::GetFrontendSpectrumData",
5      params: {
6          coreID: 0,
7          fStartHz: AAAAAAAA...AAAAAAAA...AAAAA...AAAAA...AAAAA...
8          fStopHz: 1000,
9          fftSize: 1024,
10         gain: 1,
11         numOfSamples: 256
12     }
13 }
```

# Overflow in MIPS

- ▶ Change program flow
- ▶ MIPS Architecture
  - ▶ Real-time OS
  - ▶ No stack protection
  - ▶ No memory randomization
- ▶ Exploit through Return Oriented Programming

## Wide open websockets

- ▶ Spectrum Analyzer is hosted on LAN
- ▶ Server doesn't check parameters.
- ▶ ... also, websockets are not covered by CORS anyway

## Shell Access

```
$ ls
!
dir          ?           REM          call          cd
ls           find_command   help         history       instances
system_time  man          pwd          sleep         syntax
-----
con_high     cpuLoad      cpuUtilization exit          mbufShow
memShow      mtu          mutex_debug   ping          poll
poll_print   poll_reset   poll_start    poll_stop    read_memory
reset        routeShow    run_app      shell         socket_debug
stackShow    taskDelete   taskInfo     taskPrioritySet taskResume
taskShow     taskSuspend  taskSuspendAll taskTrace    usfsShow
version      write_memory zone          taskTrace
-----
[CmRgMsgPipe] [Console] [HeapManager] [HostDqm] [cm_hal] [docsis_ctl] [dtp]
[embedded_target] [emc] [emta] [event_log] [fam] [flash] [forwarder]
[ftpLite] [httpClient] [ip_hal] [itc_hal] [msgLog] [non-vol] [pingHelper]
[pnm] [power] [snmp] [snoop] [spectrum_analyzer] [thermal]
```

Figure 4: Read, Write, Call commands

## Shell Access

Figure 5: Read, Write, Call commands

# Spectrum Analyzer is Everywhere

- ▶ Spectrum Analyzer is Reference Software written by Broadcom
  - ▶ Given to manufacturers as "inspiration"
  - ▶ Found in Technicolor, Netgear, Sagemcom, Compal, Arris, TP-Link, so far...
  - ▶ Arris flagship models SB8200 & SB6183
  - ▶ Netgear CM1000
- ▶ Conservative estimate: 100 million
- ▶ Others estimates from 500 million to 1 billion

# Fixing Cable Haunt

- ▶ Responsible disclosure
- ▶ Risk of getting out of hand
- ▶ Public disclosure

"Everyone can be hacked..."

# Key Takeaways - Responsibility

- ▶ Differing levels responsibility
  - ▶ Firmware
  - ▶ Config
  - ▶ Even custom firmware
  - ▶ ... and some probably haven't done anything
- ▶ Everybody makes mistakes
  - ▶ Know this, and be prepared to fix them!
  - ▶ Take responsibility for your system
  - ▶ Have procedures in place to fix them
  - ▶ The more you do it - the easier it gets
  - ▶ Fail gracefully

## Key Takeaways - Reachability

- ▶ Expected positive and serious response
  - ▶ Infallible until proven otherwise
  - ▶ At least a 40 page report
  - ▶ "We can prove it is not our fault"
  - ▶ Ignore it and it will go away-culture
- ▶ What you can learn
  - ▶ Be reachable - Security.txt
  - ▶ Create president for being worth contacting
    - ▶ We do this for free
  - ▶ Help contact the rest of your industry
    - ▶ Something nobody did for us
  - ▶ If you do this, they will contact you first next time

## Key Takeaways - Public disclosure

- ▶ Public disclosure makes companies take it seriously
- ▶ What you can learn
  - ▶ It is a shame - Responsible disclosure should be better
  - ▶ Its going to get out
  - ▶ Open responsible disclosure program
  - ▶ Consider bug-bounty - All the cool kids does it
    - ▶ Cheapest security consultants you will ever receive
    - ▶ The hacker can actually justify their time somewhat
  - ▶ ... don't let your lawyers create the program

# Brocade Responsible Disclosure Policy

## Working with Reporters

Brocade is grateful to Reporters identifying vulnerabilities and working with us to ensure the safety of Brocade Customers.

Brocade kindly asks Reporters to not share or publicize an unresolved vulnerability with/to third parties. By following this Responsible Security Disclosure Policy, Brocade PSIRT and associated development organizations will use reasonable efforts to:

- Respond quickly and acknowledge receipt of the vulnerability report
- Provide an estimated time frame for addressing the vulnerability report
- Notify Reporters when the vulnerability has been fixed
- Notify Reporters when the fix will take time due to the complexity of testing required

Brocade agrees to not take legal actions claims against Reporters related to disclosures submitted to Brocade PSIRT providing the following:

- Reporters don't compromise the privacy or safety of our customers and the operation of Brocade products and services.
- Reporters don't cause harm to Brocade, customers, or others.
- Reporters don't violate any criminal law.
- Reporters don't publicly disclose vulnerability details before Brocade confirms completed remediation of the vulnerability

# Brocade Responsible Disclosure Policy

Brocade take legal actions against Reporters

- Reporters cause harm to Brocade
- Reporters violate criminal law.
- Reporters don't disclose vulnerability before Brocade confirms

# Question time!

Ask away!