Risks & Vulnerabilities in Enterprise Audio Visual Solutions

‘What do you mean I have to update?’

Whois:
Tibbbbz

Anthony Tippy

- Audio Visual Support Technician
- 4 years o AV/ IT experience
- IACD student at EMU
- Breaker of things / DIY
- sloth and cat enthusiast

Why the talk?

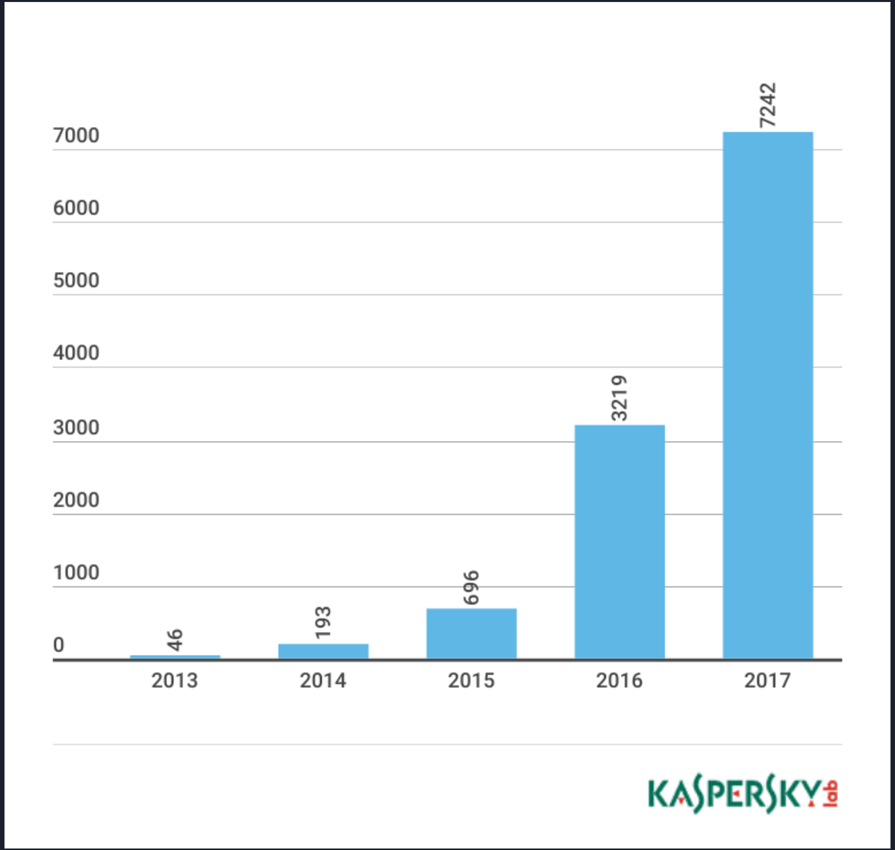
AV Devices are…

- Designed, Installed, and forgotten……………………until it breaks
- Often not considered in securing organizations
- Often Riddled with security vulnerabilities

Agenda

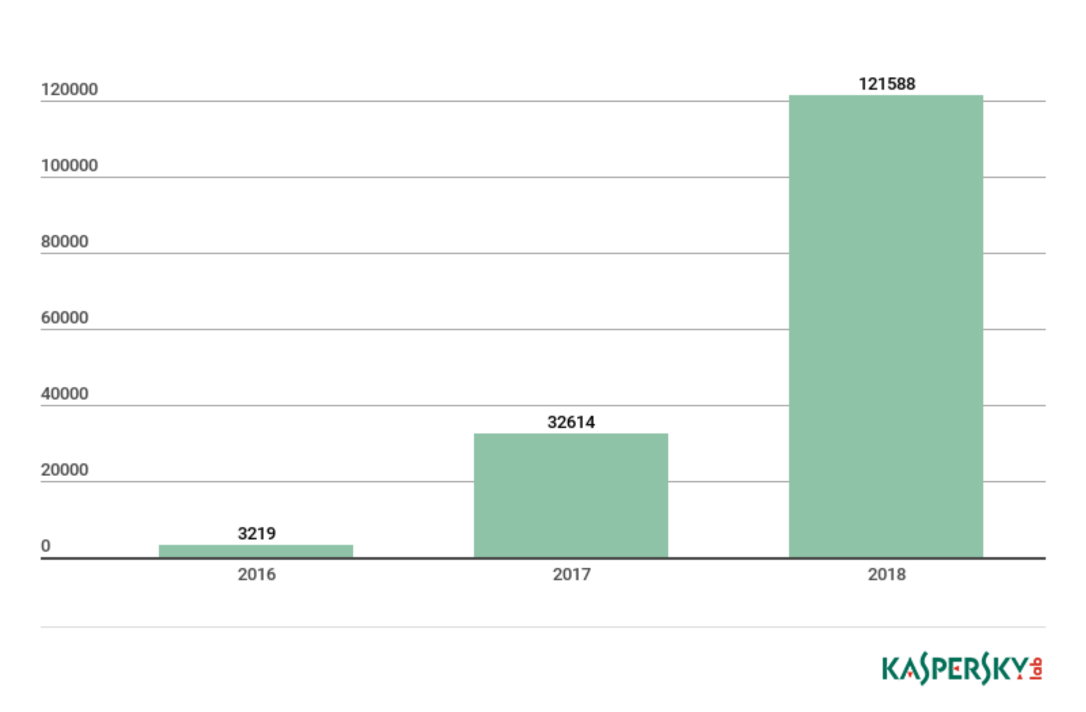
1. AV/ IOT Vulnerability Report
2. What are ‘AV Conferencing Solutions’?
3. Shodan
4. Audio Conferencing
5. Video Conferencing
6. Control Systems
7. Misc. Hardware
8. Projectors
9. Other
10. Most Vulnerable Orgs
11. How to Secure?

IOT Malware Samples



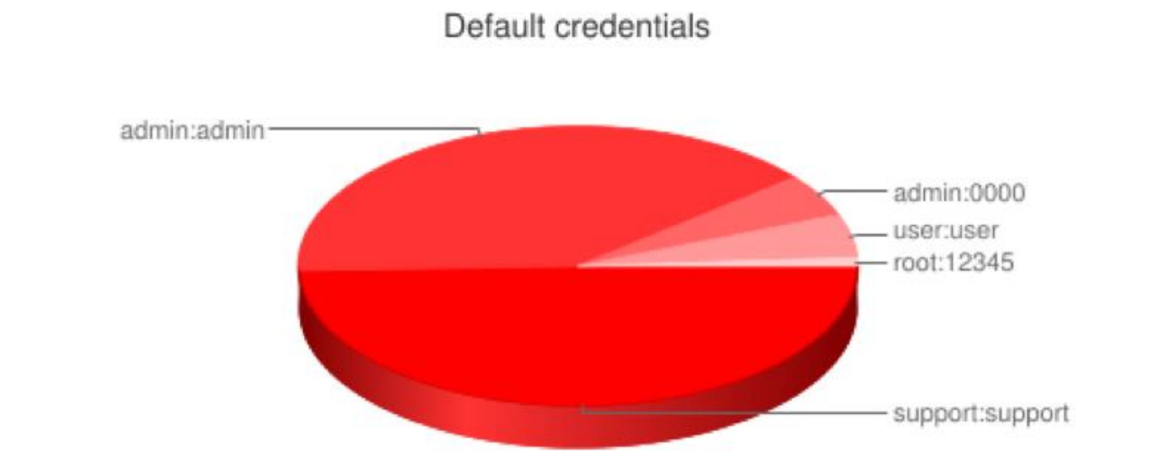
2018 IOT Malware

- devices grew three-fold in 2018 (Kaspersky Labs)
- Brute force attacks made up 93% of attacks

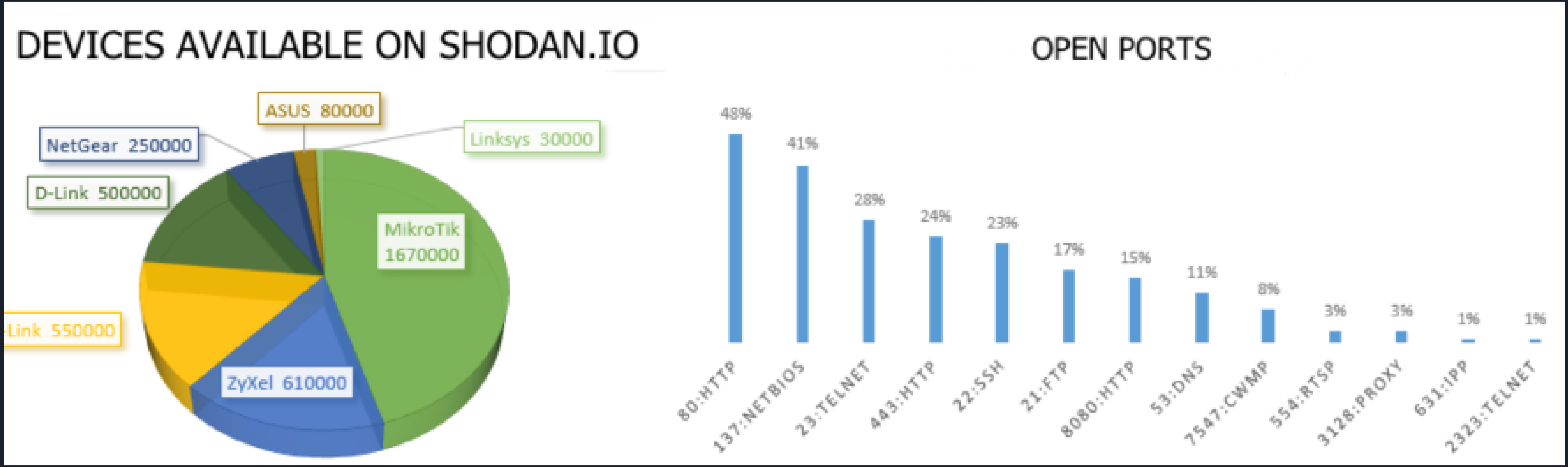


Default Passwords

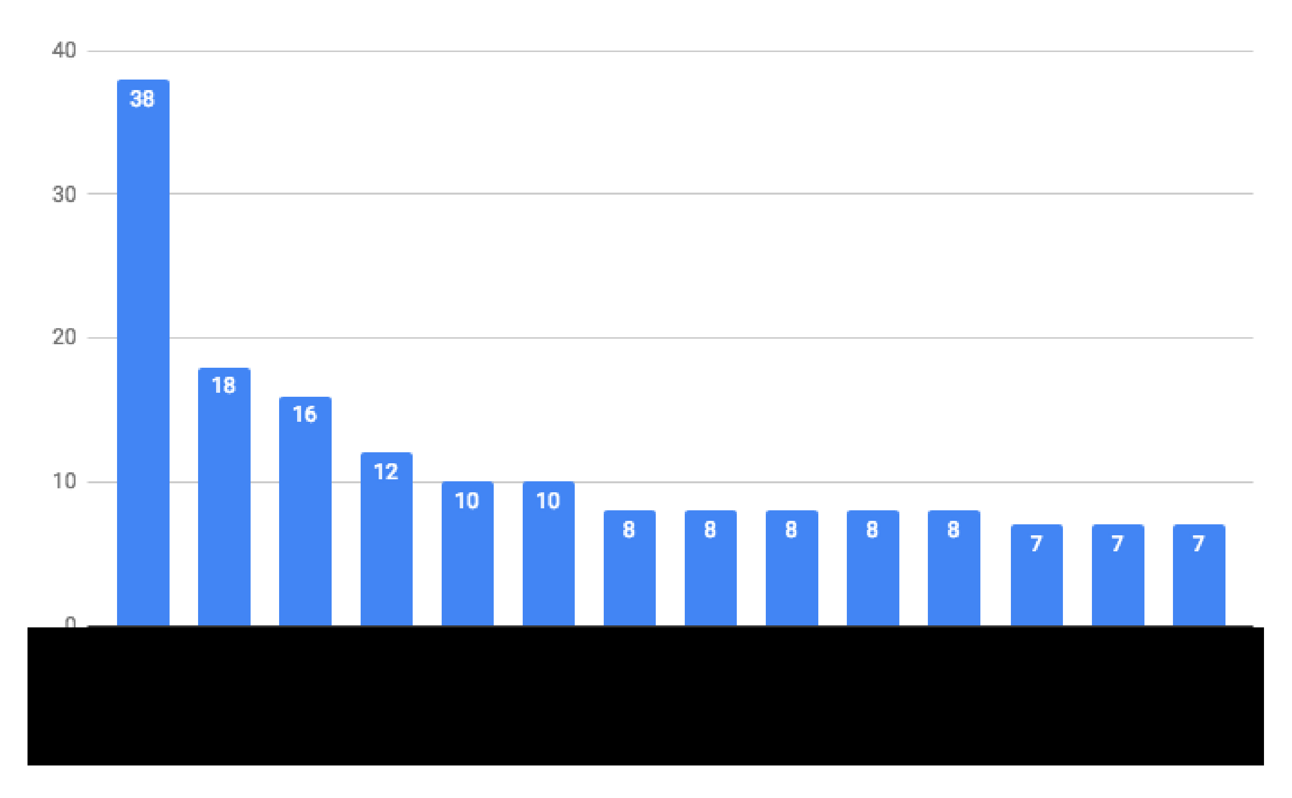
- 15% of devices have default passwords
- Top 5 username/passwords get access to 10% of devices
- “63% of data breaches use a weak, default, or stolen password.” (Verizon 2016)



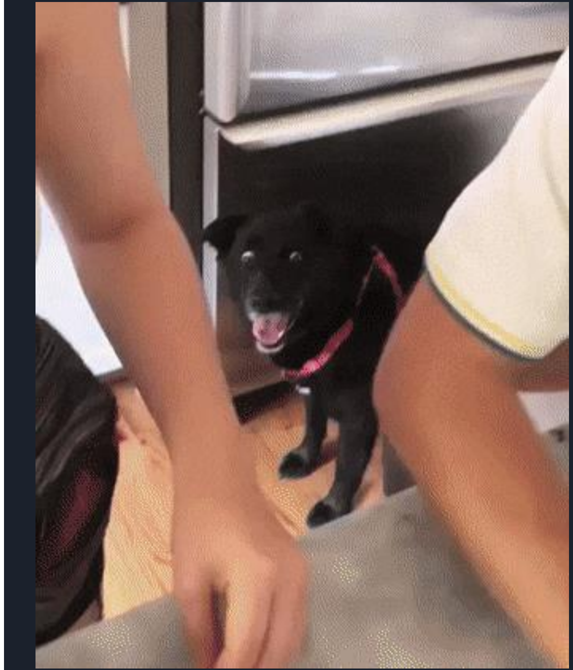
Close your ports!



There’s a lot of open ports



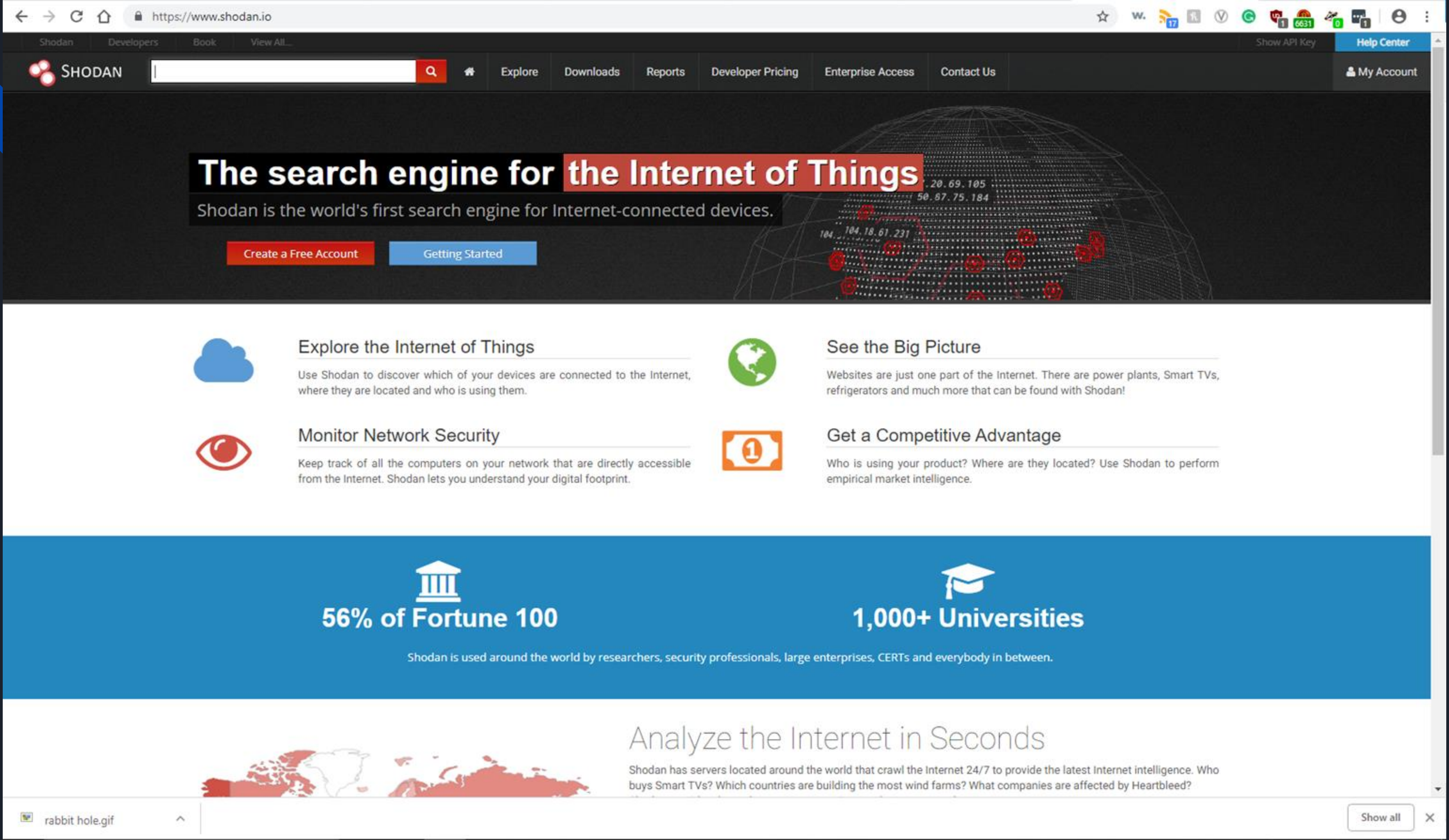
[redacted]



What are A/V Conferencing Solutions?

- Professional Displays/ Digital Signage
  - Samsung
  - LG
  - NEC
- Control Systems
  - Touch Panels
  - Master Controllers
- Phones
  - Desk Phones
  - Conference phones
  - Digital Signal Processors
- Video Conferencing Systems
  - Cisco
  - Polycom
- Misc Hardware Devices
  - Switchers/ scalers
  - Transmitters/ Receivers
  - Misc Processors

CRESTRON®
NEC
Cisco webex
AMX® by HARMAN
SAMSUNG
Polycom®
BIAMP® SYSTEMS
cisco
SERVICE SUPPORT SOLUTIONS 3
Extron®
SHARP
LG
SHURE
EPSON
EXCEED YOUR VISION



The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

56% of Fortune 100

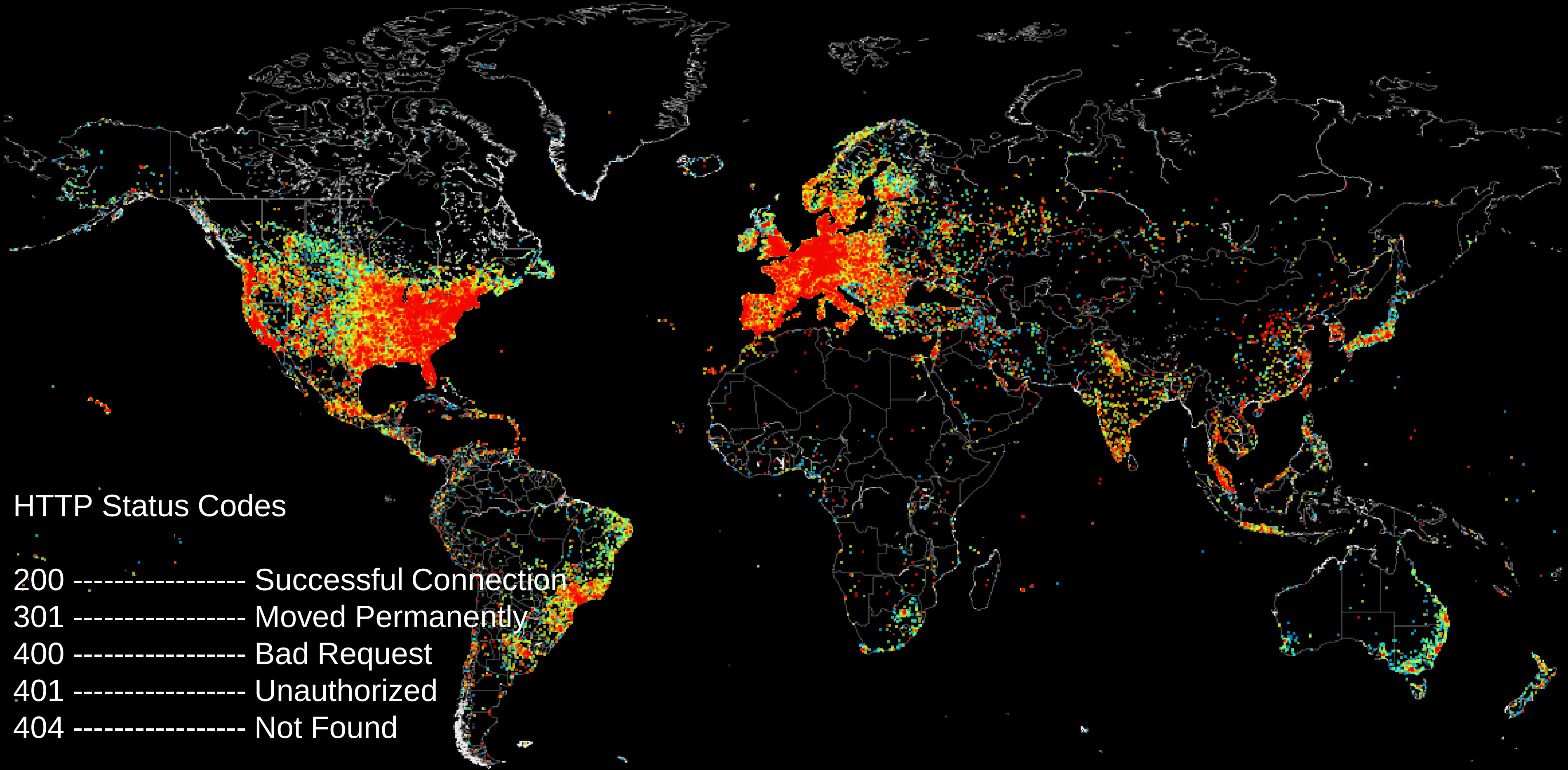
1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Analyze the Internet in Seconds

Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence. Who buys Smart TVs? Which countries are building the most wind farms? What companies are affected by Heartbleed?

SHODAN

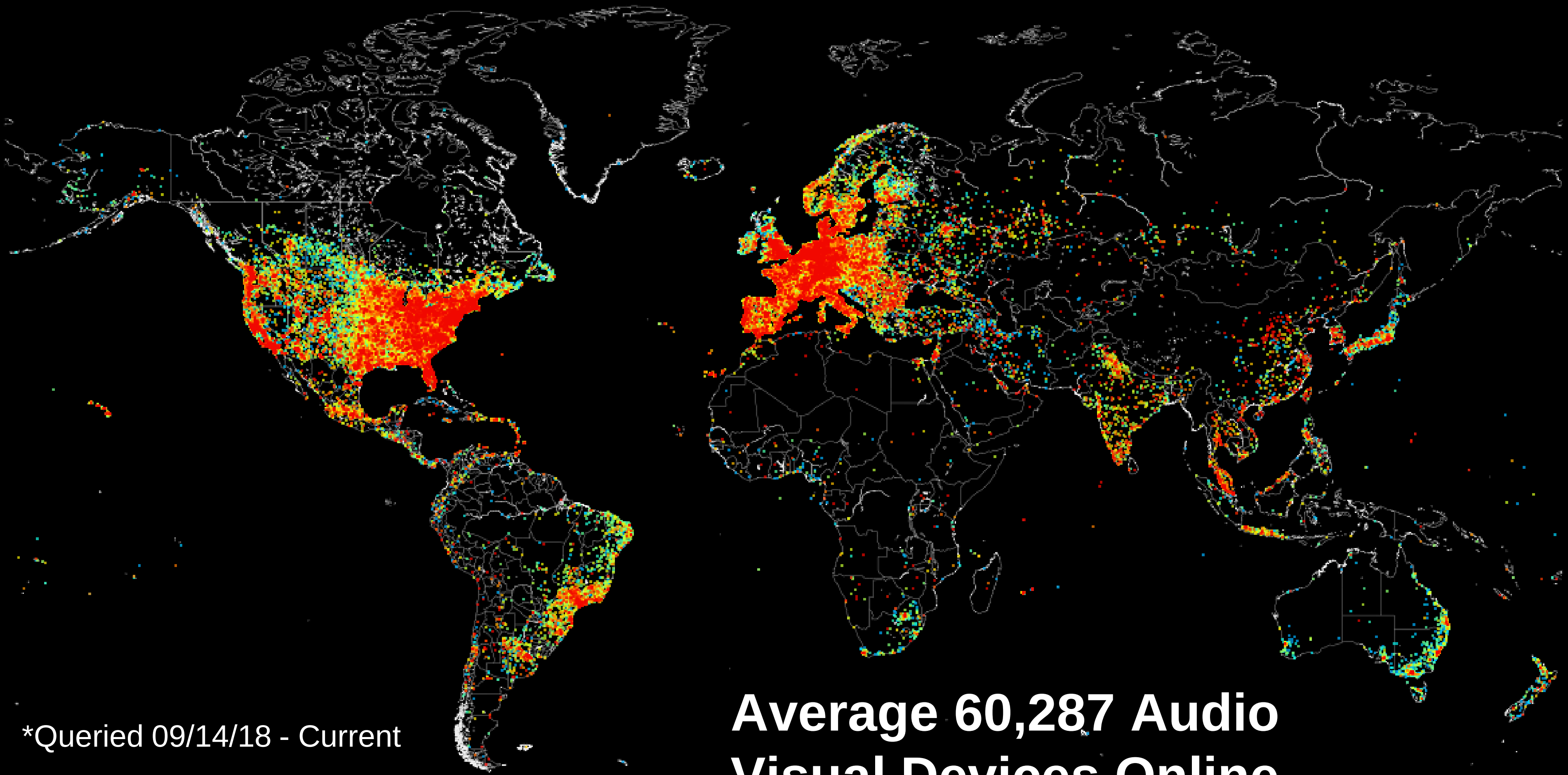


HTTP Status Codes

200	Successful Connection
301	Moved Permanently
400	Bad Request
401	Unauthorized
404	Not Found

Down the rabbit hole!

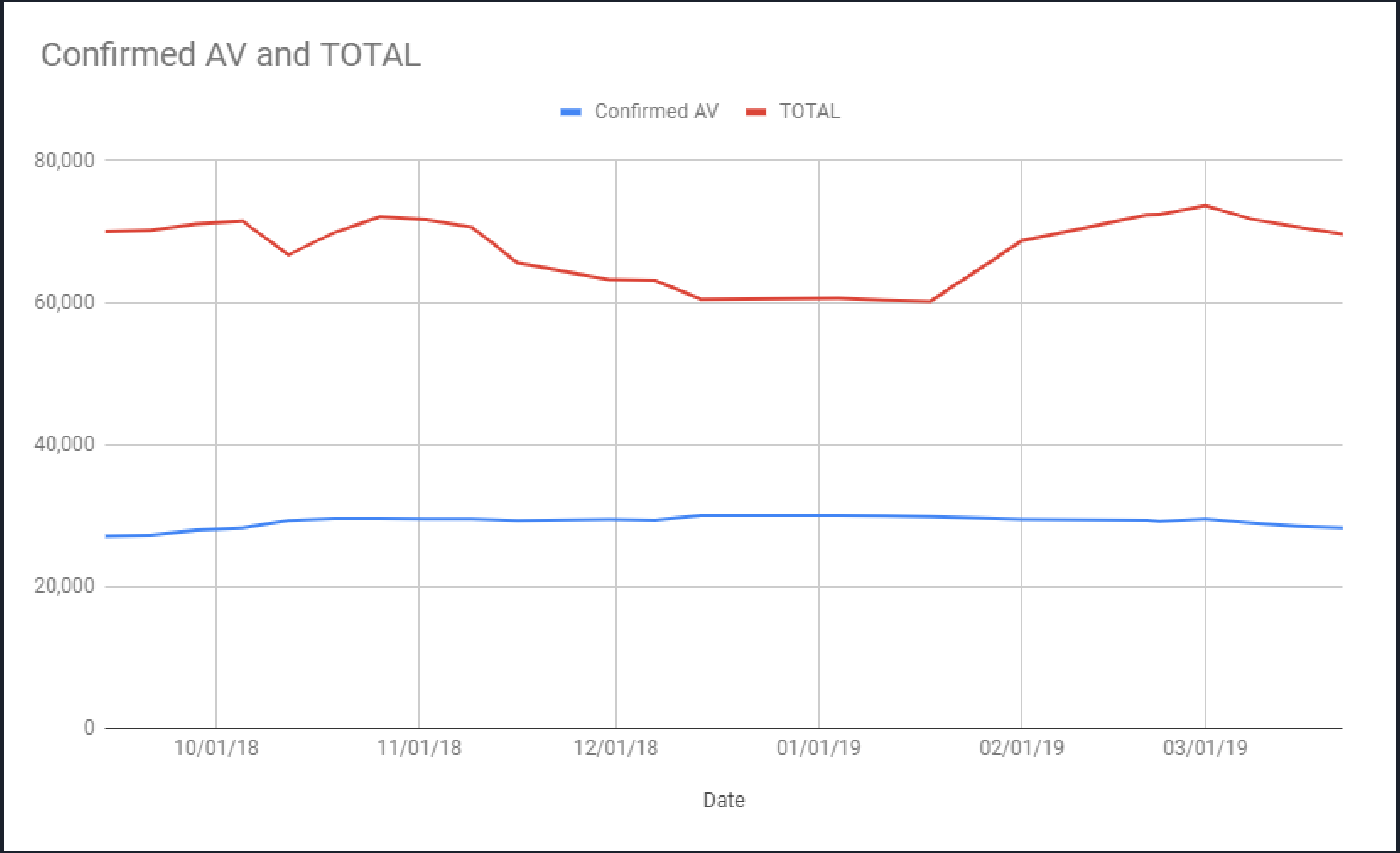
SHODAN



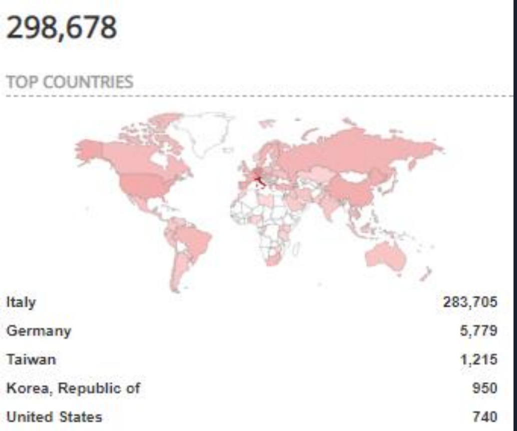
*Queried 09/14/18 - Current

Average 60,287 Audio Visual Devices Online

Not all data is the same...



Audio Conferencing- VOIP



298,678

TOP COUNTRIES

Italy	283,705
Germany	5,779
Taiwan	1,215
Korea, Republic of	950
United States	740

VoIP Services

- ATA - Analogue Telephone Adapter
- IP Phones
- PC - to - PC

Popular VoIP Protocols

- ***Session Initiation Protocol (SIP)***
- H.248 - control of switched networks
- T.38 - Fax
- Real-Time Transport Protocol (RTP)
- Skype Protocol

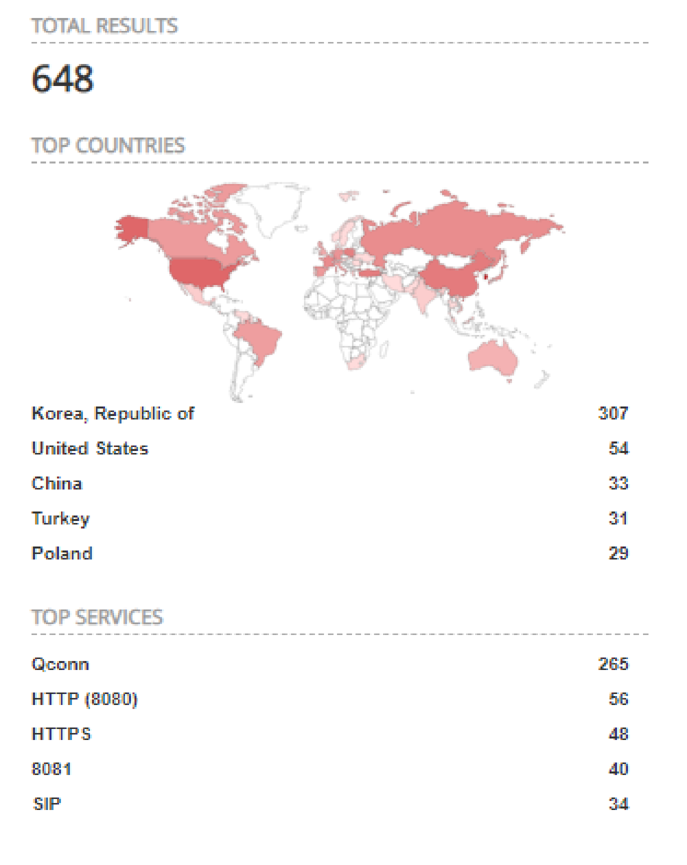
Popular VOIP Attacks

- **Eavesdropping**
  - External actors could listen in on voip communications
- **DDOS**
  - Greatest threat to enterprise systems
  - Widespread disruption of VOIP systems
- **Masquerading**
  - Impersonate user, device, or service to gain access
- **Toll fraud**
  - Actor accesses phone system to make fraudulent calls
- **Spoofing**
  - Caller ID spoofing to appear to be a legitimate number or source

DDOS Your Conference! (CVE 2018-0325)

- Cisco 7800, 8800, and 8821 series phones
- SIP vulnerability
- ***No patch as of Aug 2018***
- 8800 Series phones could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected phone
- Stop all the productivity!

IP-Phone-Web GUI’s



TOTAL RESULTS

648

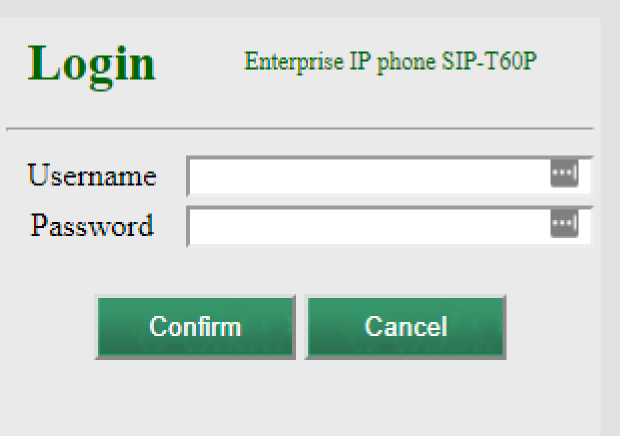
TOP COUNTRIES

Korea, Republic of	307
United States	54
China	33
Turkey	31
Poland	29

TOP SERVICES

Qconn	265
HTTP (8080)	56
HTTPS	48
8081	40
SIP	34

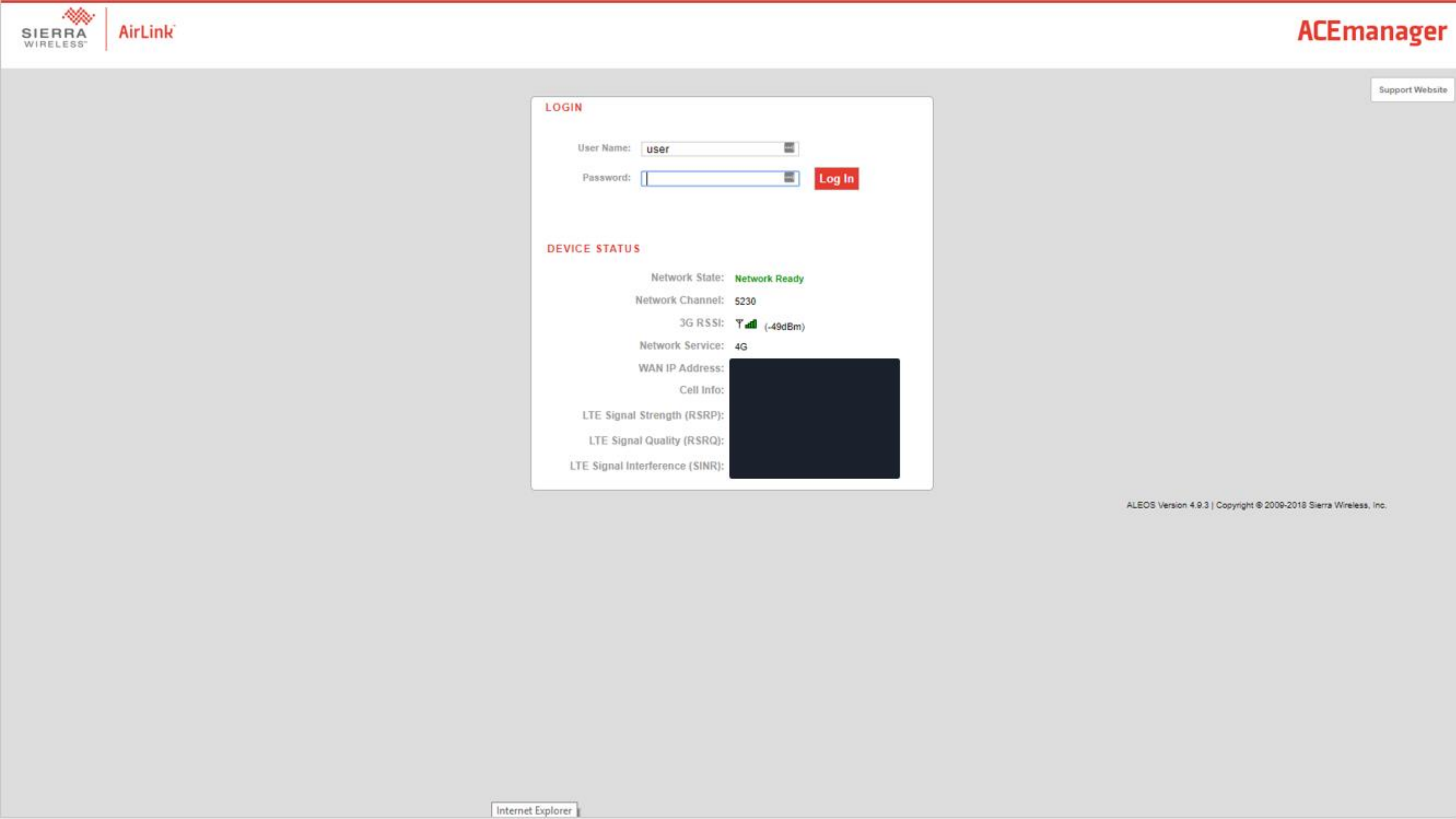
Phones, Phones, Phones...


Login

Enterprise IP phone SIP-T60P

Username

Password



LOGIN

User Name: user

Password:

DEVICE STATUS

Network State: Network Ready

Network Channel: 5230

3G RSSI: (-49dBm)

Network Service: 4G

WAN IP Address:

Cell Info:

LTE Signal Strength (RSRP):

LTE Signal Quality (RSRQ):

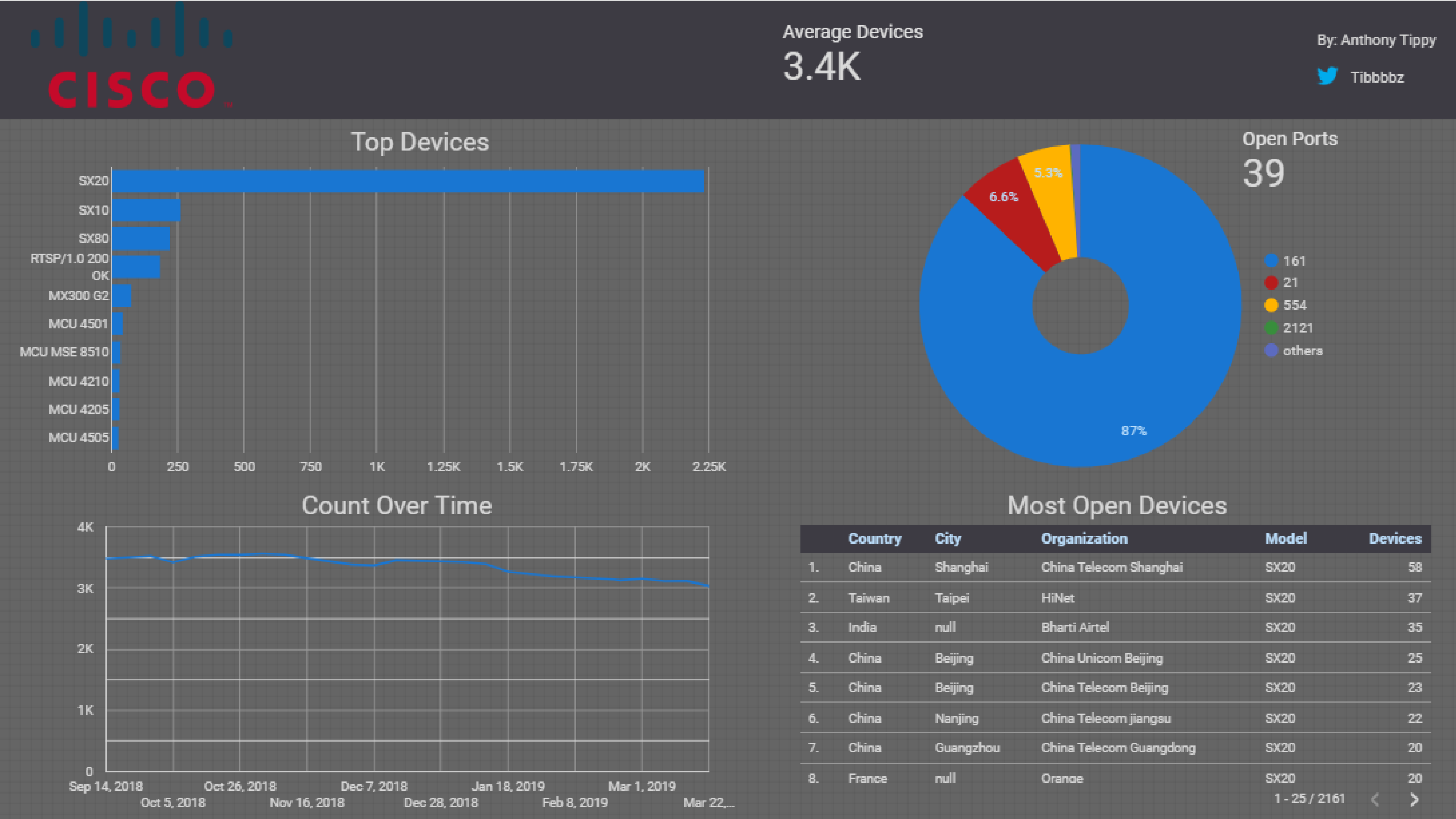
LTE Signal Interference (SINR):

[redacted]

ALEOS Version 4.9.3 | Copyright © 2009-2018 Sierra Wireless, Inc.

Video Conferencing- Cisco TelePresence

- Video Conference systems for all size organizations
- Managed with Cisco's - Device Management platform (CUCM)



Average Devices

3.4K

By: Anthony Tippy

Tibbbbz

Most Open Devices

	Country	City	Organization	Model	Devices
1.	China	Shanghai	China Telecom Shanghai	SX20	58
2.	Taiwan	Taipei	HiNet	SX20	37
3.	India	null	Bharti Airtel	SX20	35
4.	China	Beijing	China Unicom Beijing	SX20	25
5.	China	Beijing	China Telecom Beijing	SX20	23
6.	China	Nanjing	China Telecom jiangsu	SX20	22
7.	China	Guangzhou	China Telecom Guangdong	SX20	20
8.	France	null	Orange	SX20	20

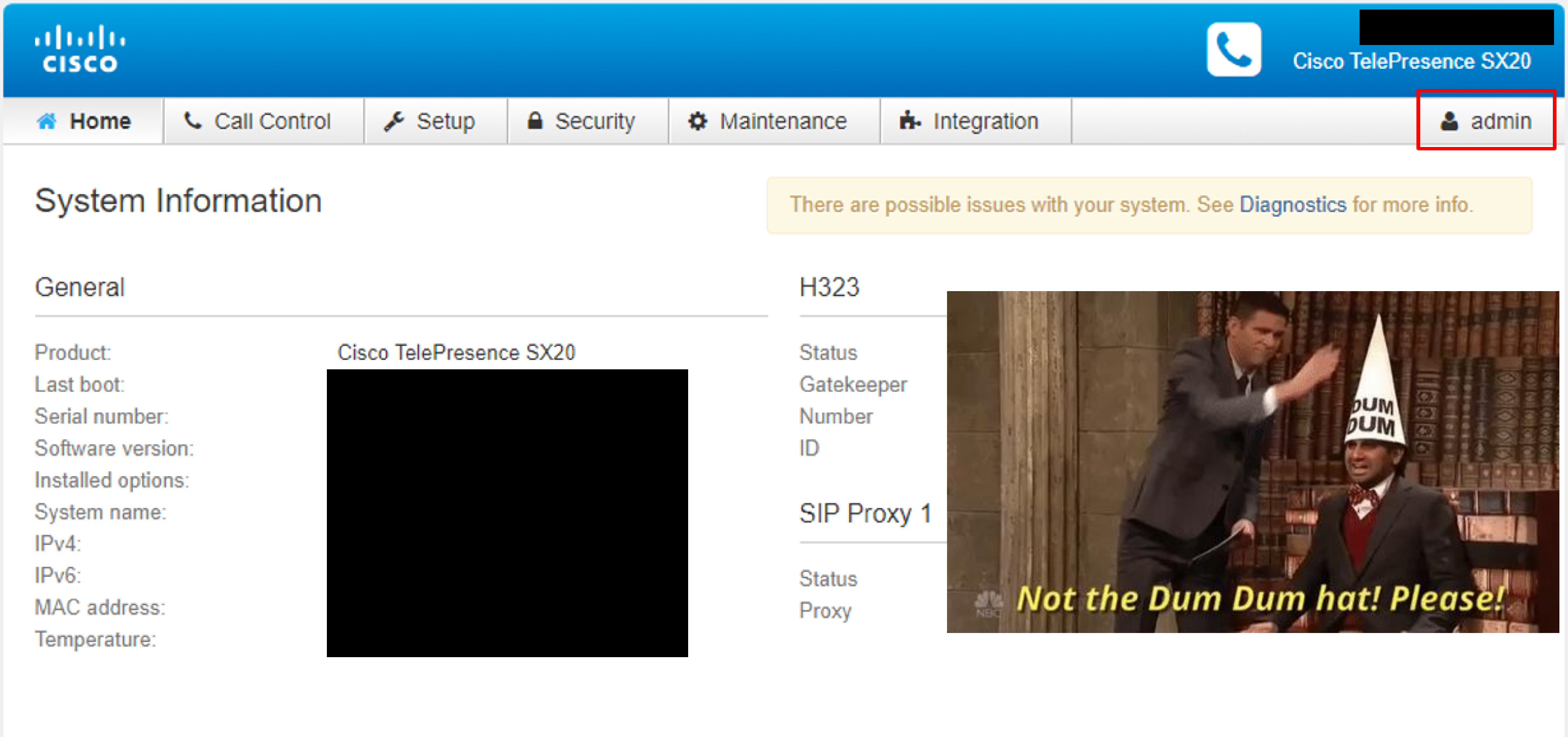
1 - 25 / 2161

CVE-2018-5391- FragmentStack (Linux DDOS)

- Linux 3.9 vulnerability
- Linux kernel is affected by the IP Fragment Reassembly Denial of Service

Affected Devices

- Cisco EX series
- Cisco Integrator C Series
- MX Series
- Profile Series
- SX80 codec
- WebEx Roomkit



System Information

There are possible issues with your system. See Diagnostics for more info.

General

Product: Cisco TelePresence SX20
Last boot:
Serial number:
Software version:
Installed options:
System name:
IPv4:
IPv6:
MAC address:
Temperature:

[redacted]

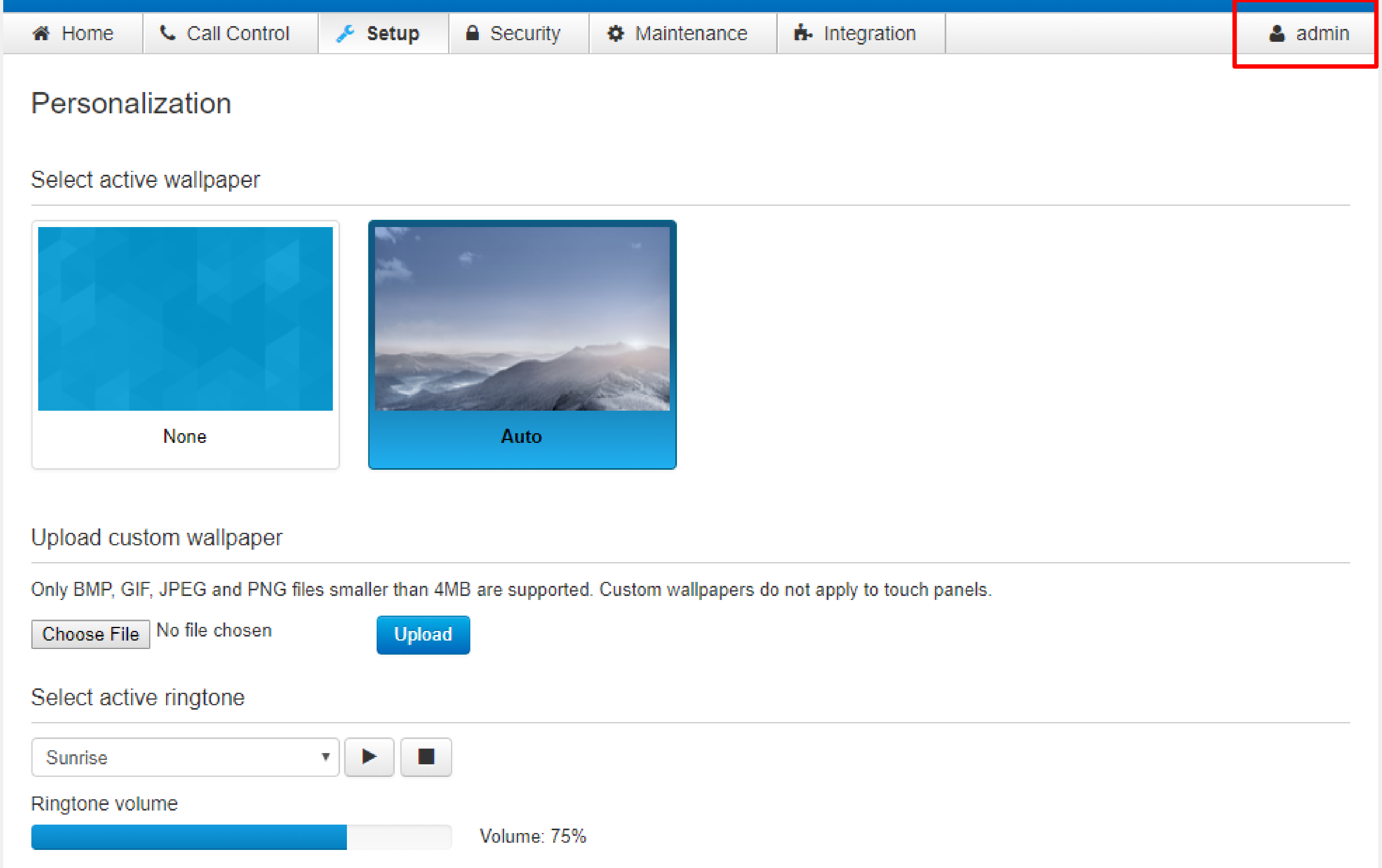
H323

Status
Gatekeeper
Number
ID

SIP Proxy 1

Status
Proxy

Not the Dum Dum hat! Please!



Personalization

Select active wallpaper

Upload custom wallpaper

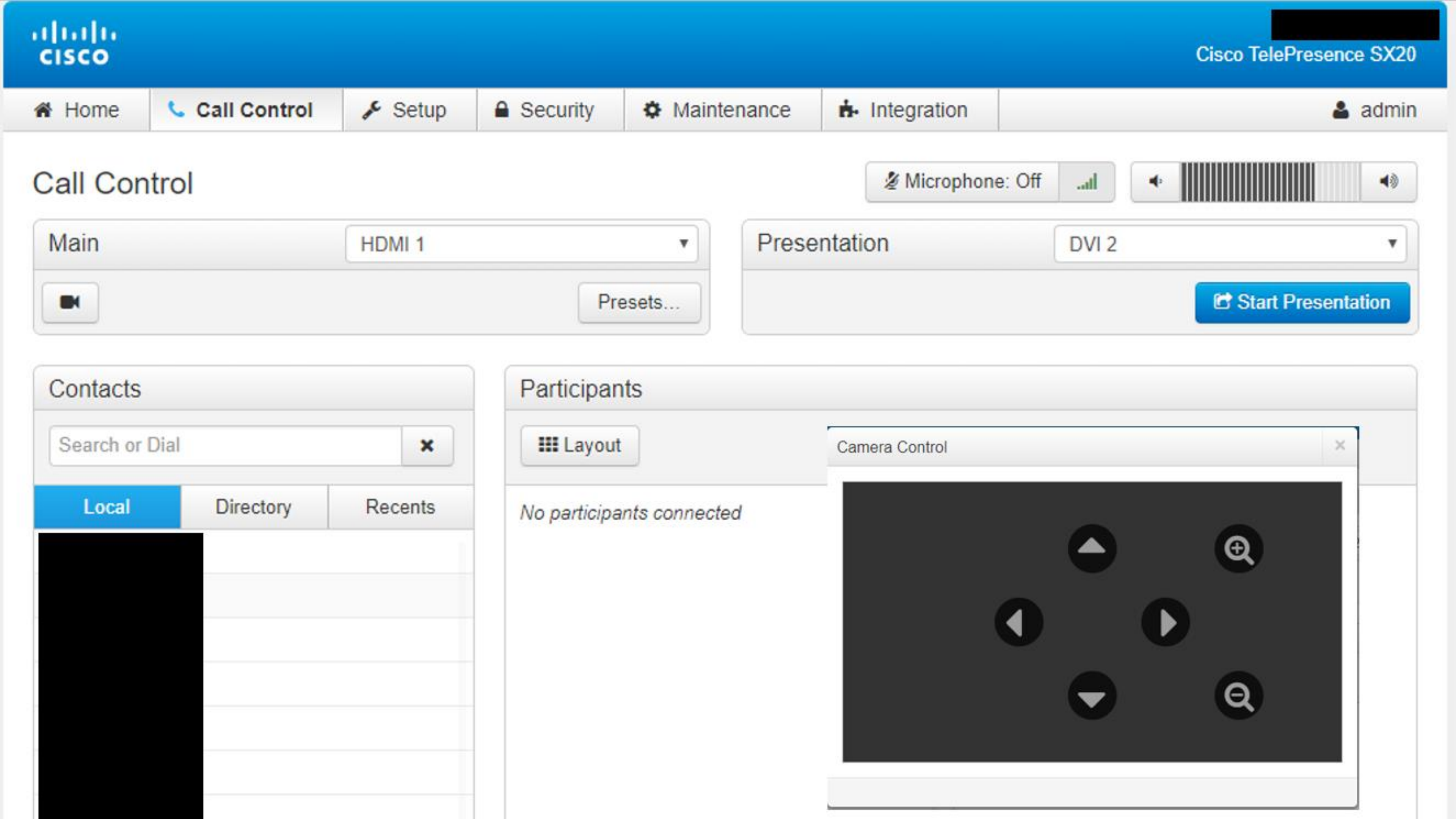
Only BMP, GIF, JPEG and PNG files smaller than 4MB are supported. Custom wallpapers do not apply to touch panels.

Select active ringtone

Sunrise

Ringtone volume

Volume: 75%



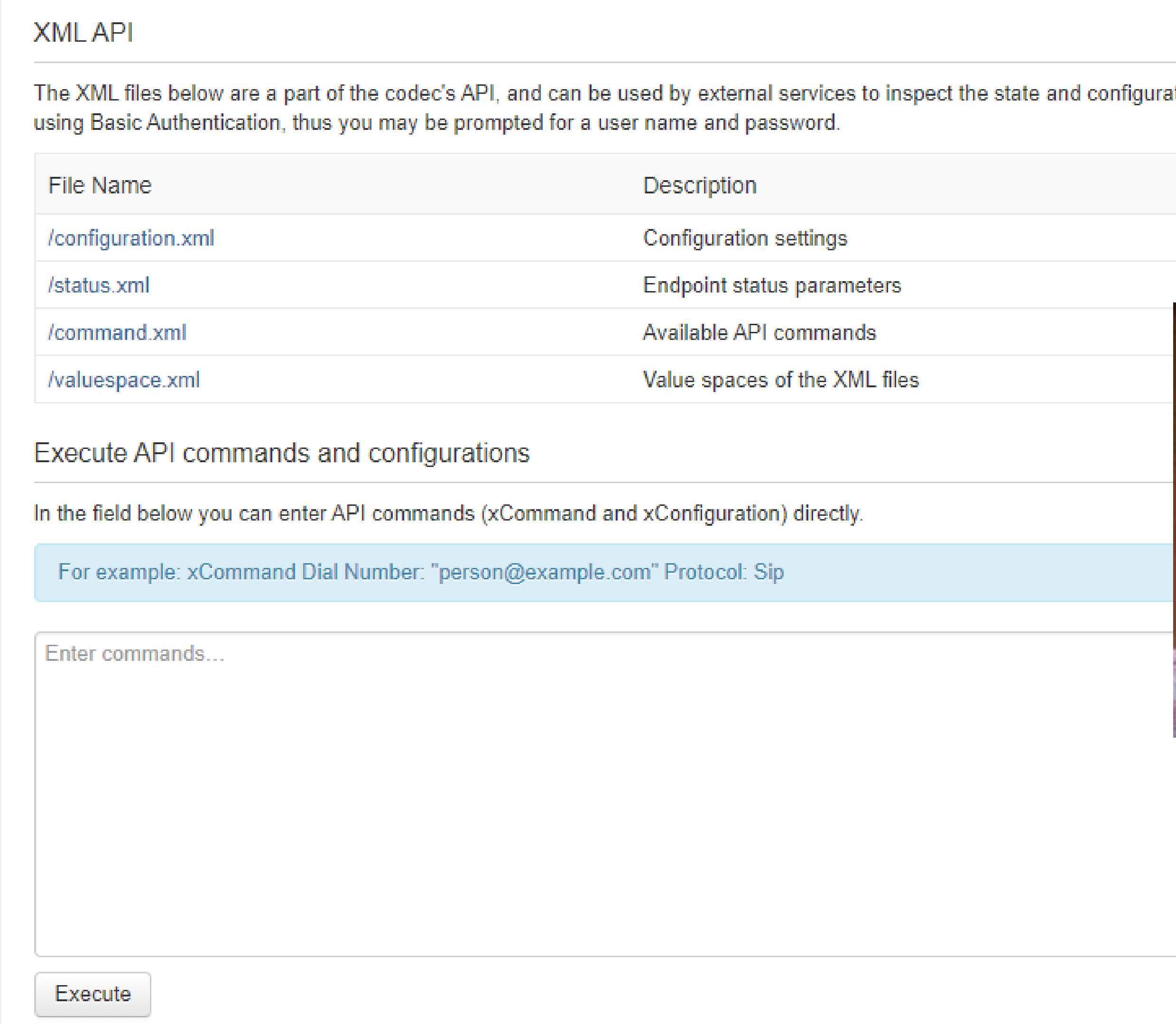
Call Control

Microphone: Off

Main: HDMI 1

Presentation: DVI 2

No participants connected



XML API

The XML files below are a part of the codec's API, and can be used by external services to inspect the state and configuration of the codec. The files are protected using Basic Authentication, thus you may be prompted for a user name and password.

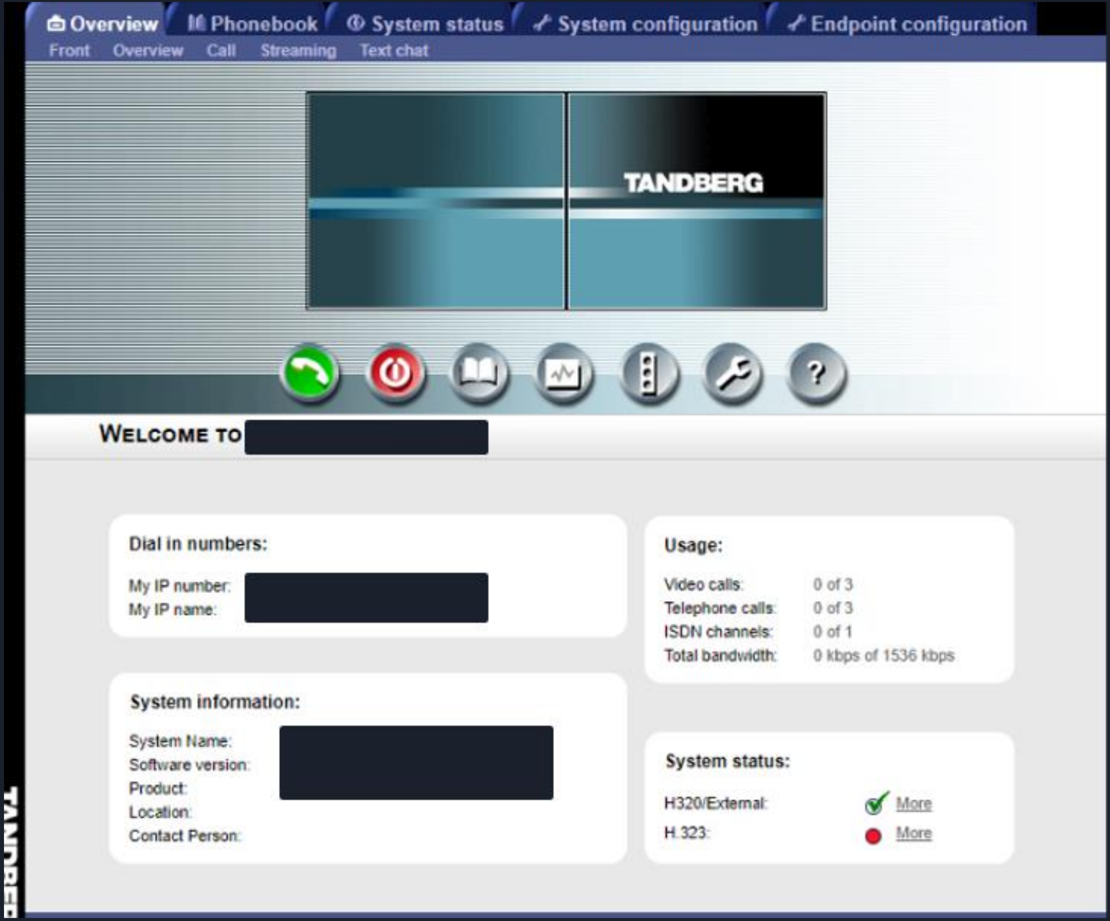
File Name	Description
/configuration.xml	Configuration settings
/status.xml	Endpoint status parameters
/command.xml	Available API commands
/valuespace.xml	Value spaces of the XML files

Execute API commands and configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

Tandberg Video Codec- 3000 MXP



Welcome to [redacted]

Dial in numbers:

My IP number:
My IP name:
[redacted]

Usage:

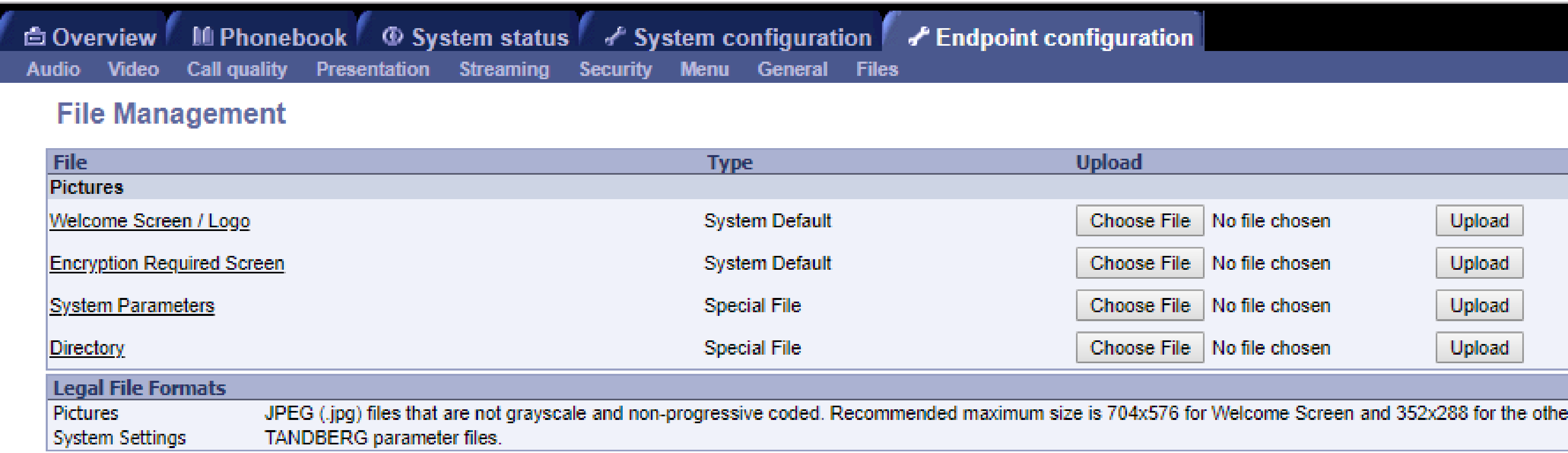
Video calls:	0 of 3
Telephone calls:	0 of 3
ISDN channels:	0 of 1
Total bandwidth:	0 kbps of 1536 kbps

System information:

System Name:
Software version:
Product:
Location:
Contact Person:
[redacted]

System status:

H320/External:	✓	More
H.323:	●	More

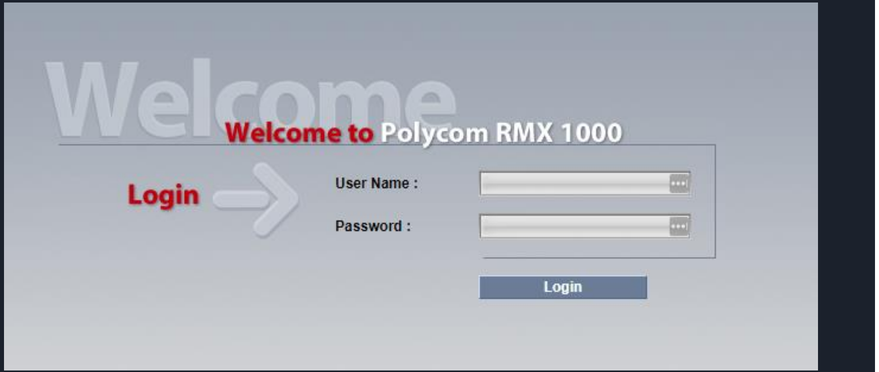


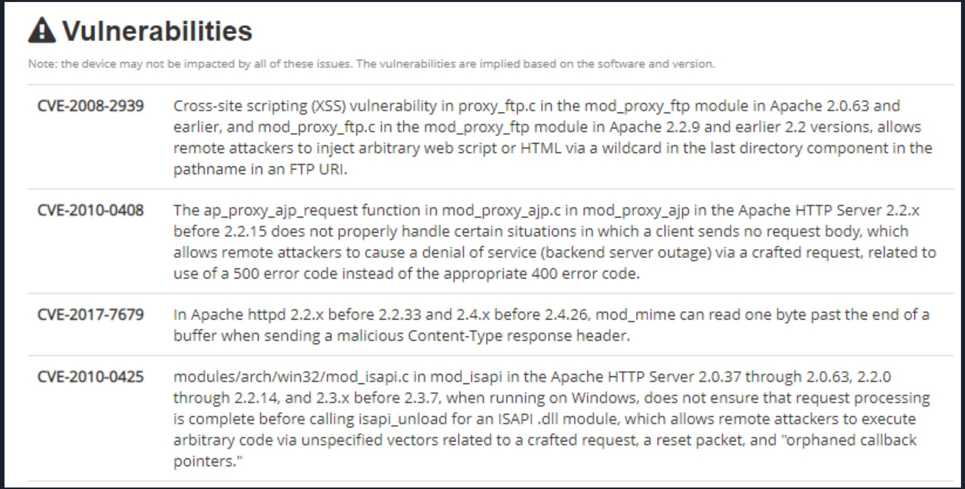
File Management

File	Type	Upload		
Pictures				
Welcome Screen / Logo	System Default	Choose File	No file chosen	Upload
Encryption Required Screen	System Default	Choose File	No file chosen	Upload
System Parameters	Special File	Choose File	No file chosen	Upload
Directory	Special File	Choose File	No file chosen	Upload

Legal File Formats	
Pictures	JPEG (.jpg) files that are not grayscale and non-progressive coded. Recommended maximum size is 704x576 for Welcome Screen and 352x288 for the othe
System Settings	TANDBERG parameter files.

Polycom Audio Video Call Systems





⚠ Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2008-2939	Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.
CVE-2010-0408	The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2010-0425	modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

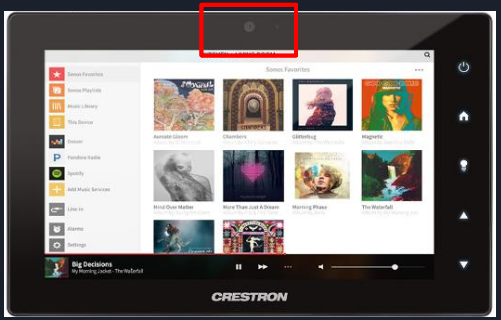
Control Systems

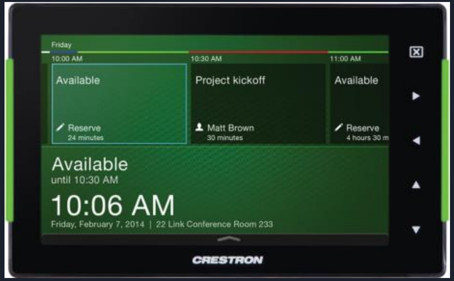
- Used in..
  - Universities
  - Enterprises
  - Home Automation
  - Hotels
  - Airports

Popular Vendors

- AMX
- Cisco
- Crestron
- Extron

Crestron Touch Panels (TSW Series)

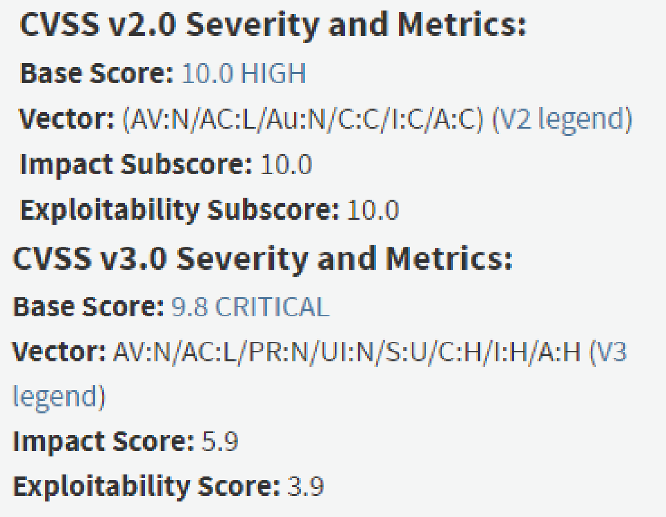




- Hotels/ Conference Centers
- Universities
- Airports
- Home Automation
  - Lights
  - Home Security
  - Music/ Video
- Conference room control panel
  - Inputs
  - Audio Conference/ Video
- Conference Room Scheduler
  - Integrates with Exchange. Office 365, G Suite..etc
- Built in Camera/ Mic

CVE-2018-10630 - Passwords!

- Crestron TSW-X60 Series
  - Models Affected
    - TSW- 1060
    - TSW- 560
    - TSW- 760
    - And MC3 Controller
- RCE/ Low skill level
- Shipped with No Authentication (CTP)
- ***ALL*** versions prior to 2.001.0037.001 affected
- Credit to: *Jackson Thuraisamy* & *Ricky Lawshae* for initial discovery



CVSS v2.0 Severity and Metrics:

Base Score: 10.0 HIGH

Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)

Impact Subscore: 10.0

Exploitability Subscore: 10.0

CVSS v3.0 Severity and Metrics:

Base Score: 9.8 CRITICAL

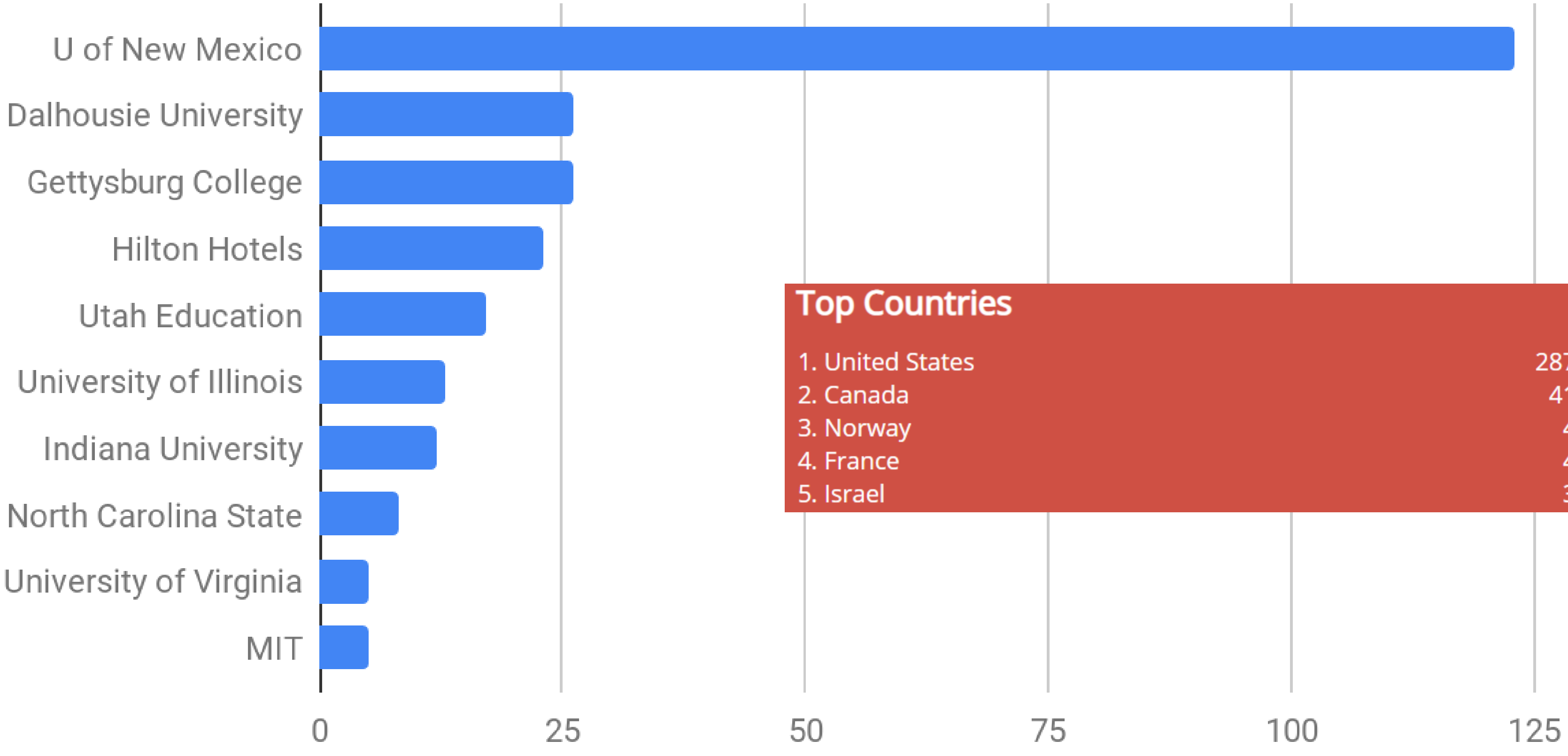
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)

Impact Score: 5.9

Exploitability Score: 3.9

TSW-X60 - Top Organizations

Total: 313



Top Countries

1. United States	287
2. Canada	41
3. Norway	4
4. France	4
5. Israel	3

CRESTRON. TSW -X60 Touch Panels

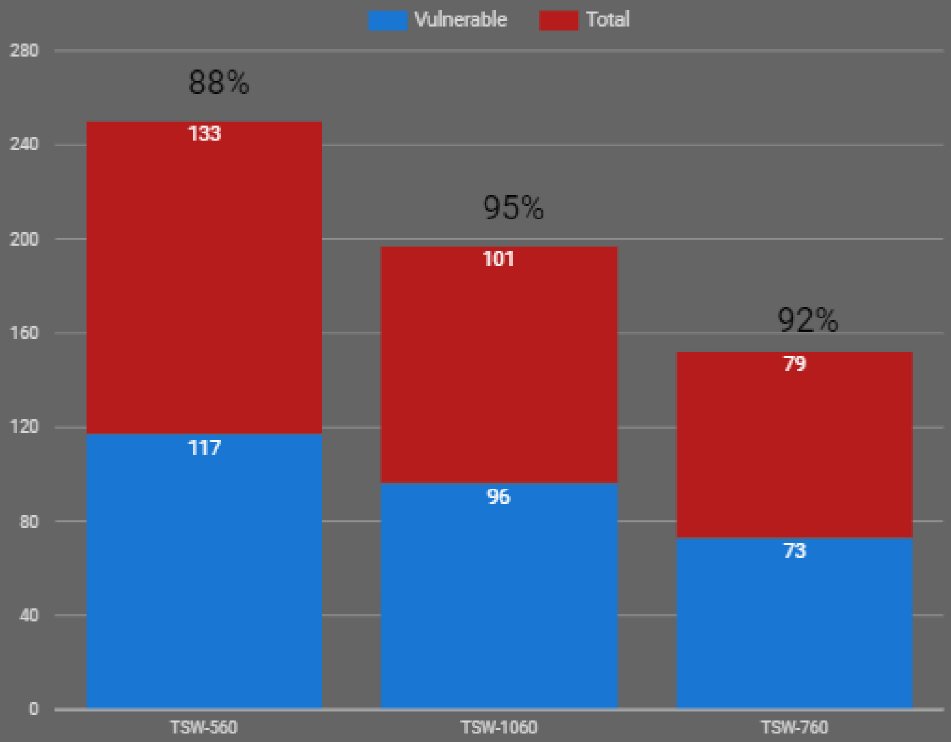
By: Anthony Tippy

Tibbbbz

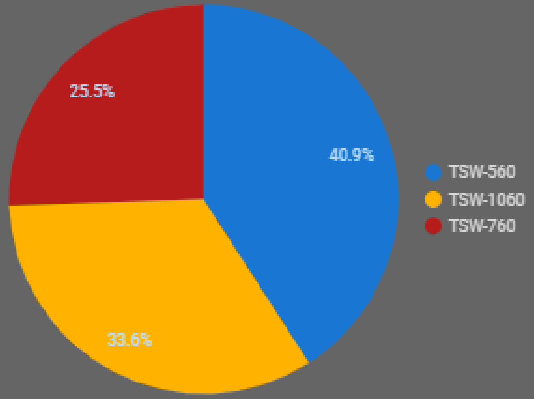
Total Devices

313

CVE-2018-10630- No CTP Authentication



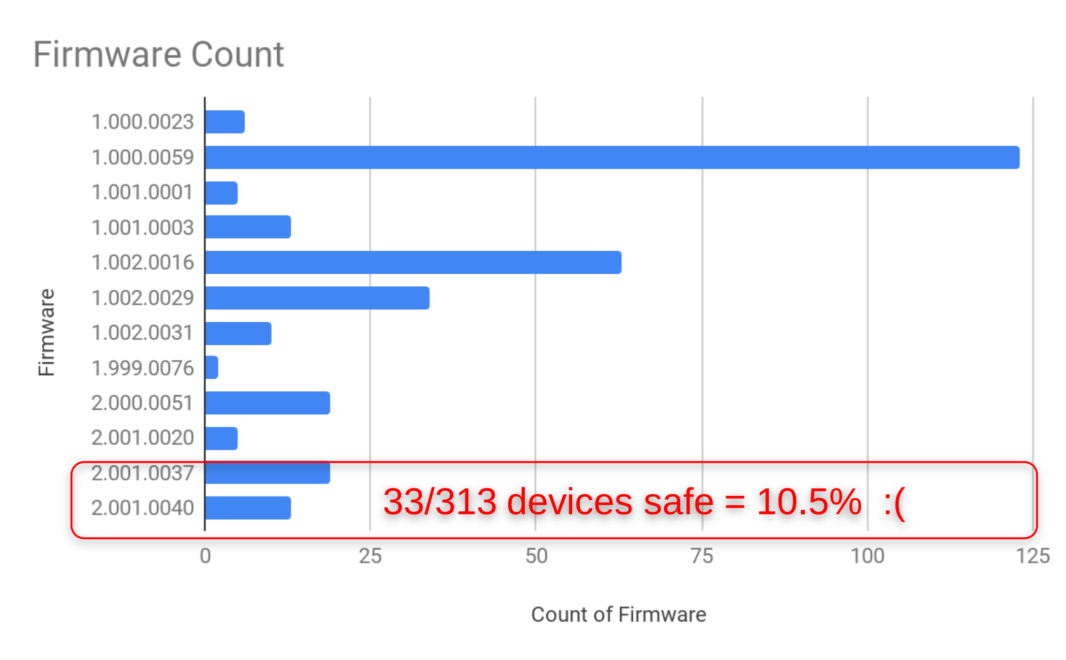
Vulnerable Touch Panels



	Model	Version	Version
1.	TSW-560	1.000.0059	85
2.	TSW-1060	1.002.0029	30
3.	TSW-760	1.002.0016	23
4.	TSW-1060	1.002.0016	23
5.	TSW-1060	1.000.0059	23
6.	TSW-560	1.002.0016	17
7.	TSW-760	2.000.0051	16
8.	TSW-760	1.000.0059	15

1 - 25 / 26 ‹ ›

UPDATE YOUR DEVICES PLS

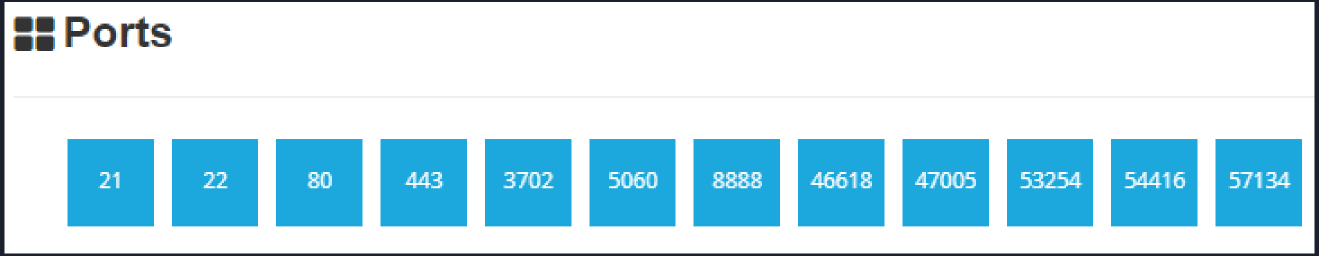


33/313 devices safe = 10.5% :(

Update
YOUR
DEVICES!

Lets see what we can find!

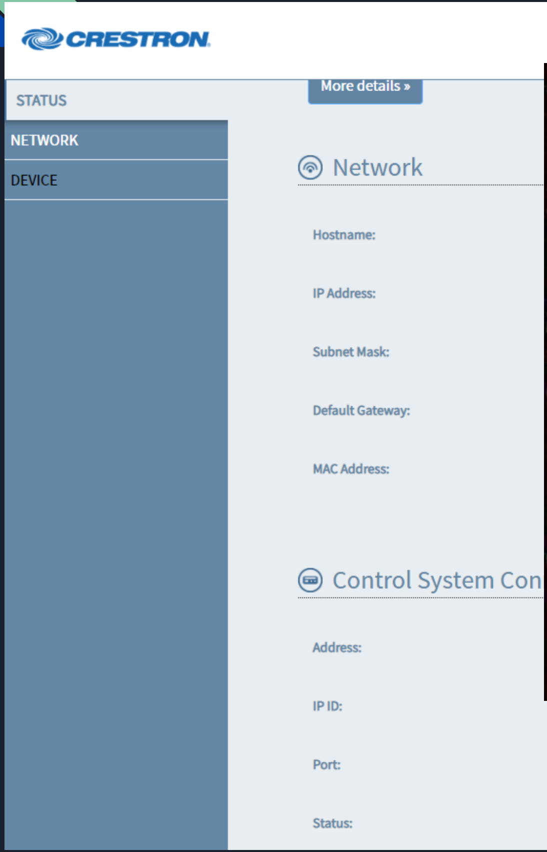
- FTP, SSH, HTTP, HTTPS, SIP wide open
- Crestron Default Port = 41794



Ports

21 22 80 443 3702 5060 8888 46618 47005 53254 54416 57134

Make your own rules!



CRESTRON

Network

Hostname:

IP Address:

Subnet Mask:

Default Gateway:

MAC Address:

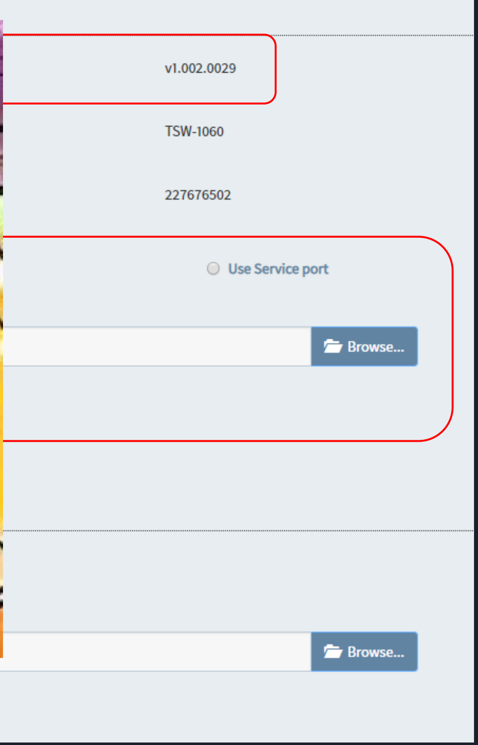
Control System Con

Address:

IP ID: 26

Port: 41794

Status: ONLINE



Firmware

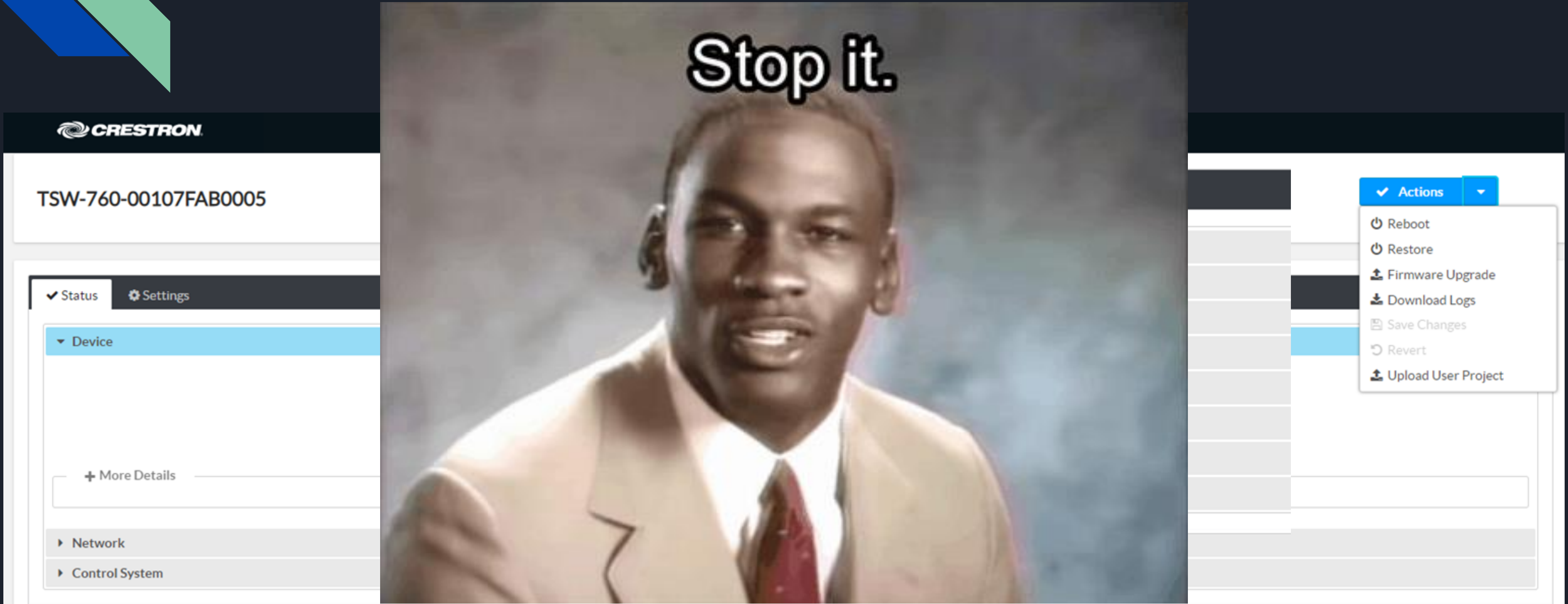
v1.002.0029

TSW-1060

227676502

○ Use Service port

Newer TSW-760- Fully Unauthenticated!



Jaw Drop

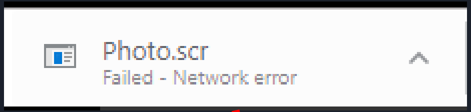
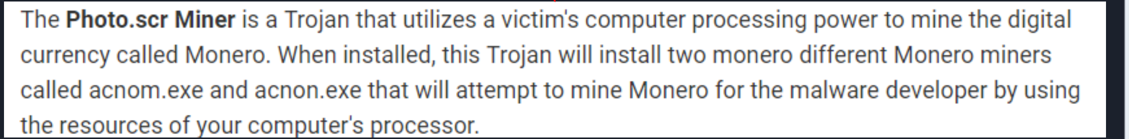
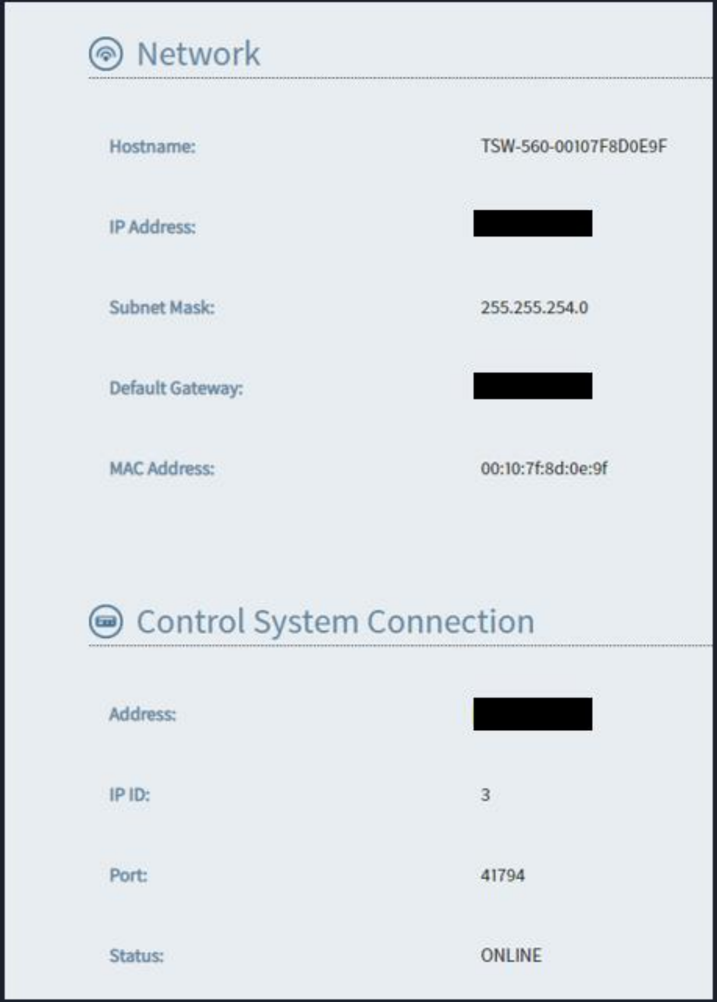


Photo.scr
Failed - Network error



The **Photo.scr Miner** is a Trojan that utilizes a victim's computer processing power to mine the digital currency called Monero. When installed, this Trojan will install two monero different Monero miners called acnom.exe and acnon.exe that will attempt to mine Monero for the malware developer by using the resources of your computer's processor.



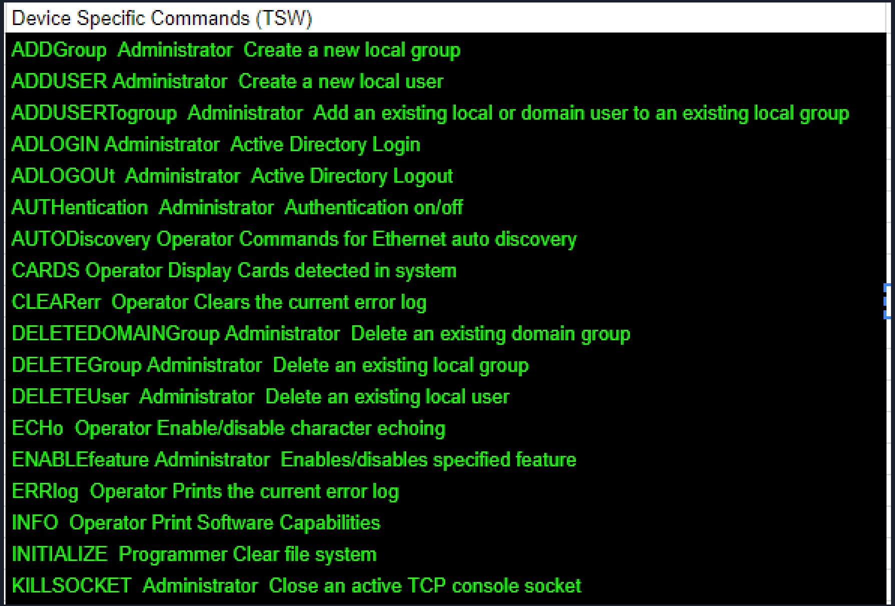
Network

Hostname:	TSW-560-00107F8D0E9F
IP Address:	[redacted]
Subnet Mask:	255.255.254.0
Default Gateway:	[redacted]
MAC Address:	00:10:7f:8d:0e:9f

Control System Connection

Address:	[redacted]
IP ID:	3
Port:	41794
Status:	ONLINE

Crestron TSW telnet commands



Device Specific Commands (TSW)

ADDGroup Administrator Create a new local group

ADDUSER Administrator Create a new local user

ADDUSERTogroup Administrator Add an existing local or domain user to an existing local group

ADLOGIN Administrator Active Directory Login

ADLOGOUt Administrator Active Directory Logout

AUTHentication Administrator Authentication on/off

AUTODiscovery Operator Commands for Ethernet auto discovery

CARDS Operator Display Cards detected in system

CLEARerr Operator Clears the current error log

DELETEDOMAINGroup Administrator Delete an existing domain group

DELETEGroup Administrator Delete an existing local group

DELETEUser Administrator Delete an existing local user

ECHo Operator Enable/disable character echoing

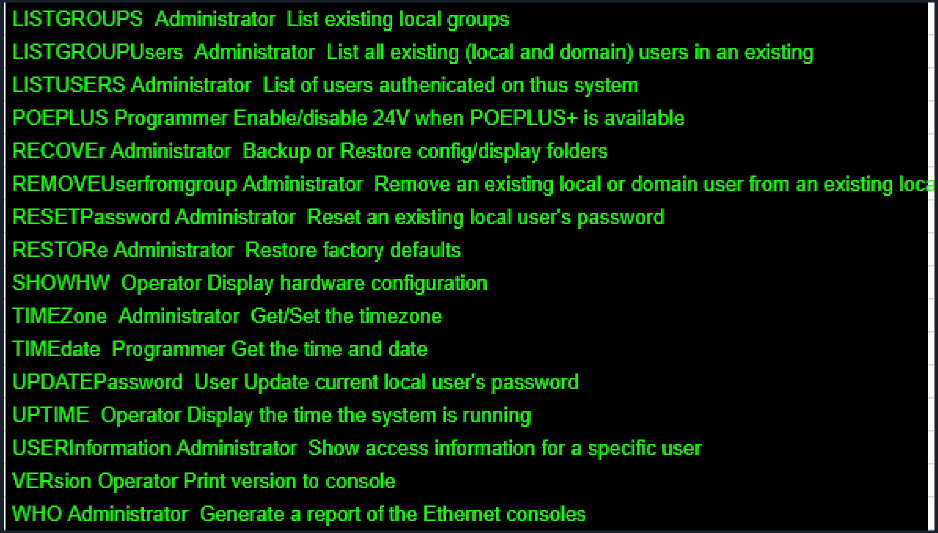
ENABLEfeature Administrator Enables/disables specified feature

ERRlog Operator Prints the current error log

INFO Operator Print Software Capabilities

INITIALIZE Programmer Clear file system

KILLSOCKET Administrator Close an active TCP console socket



LISTGROUPS Administrator List existing local groups

LISTGROUPUsers Administrator List all existing (local and domain) users in an existing

LISTUSERS Administrator List of users authenicated on thus system

POEPLUS Programmer Enable/disable 24V when POEPLUS+ is available

RECOVEr Administrator Backup or Restore config/display folders

REMOVEUserfromgroup Administrator Remove an existing local or domain user from an existing loca

RESETPassword Administrator Reset an existing local user's password

RESTORe Administrator Restore factory defaults

SHOWHW Operator Display hardware configuration

TIMEZone Administrator Get/Set the timezone

TIMEdate Programmer Get the time and date

UPDATEPassword User Update current local user's password

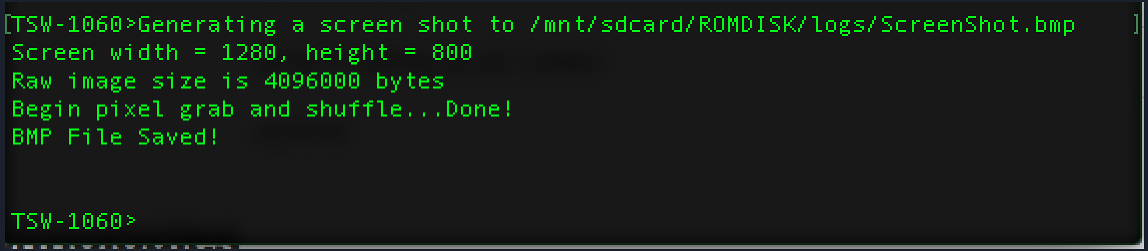
UPTIME Operator Display the time the system is running

USERInformation Administrator Show access information for a specific user

VERsion Operator Print version to console

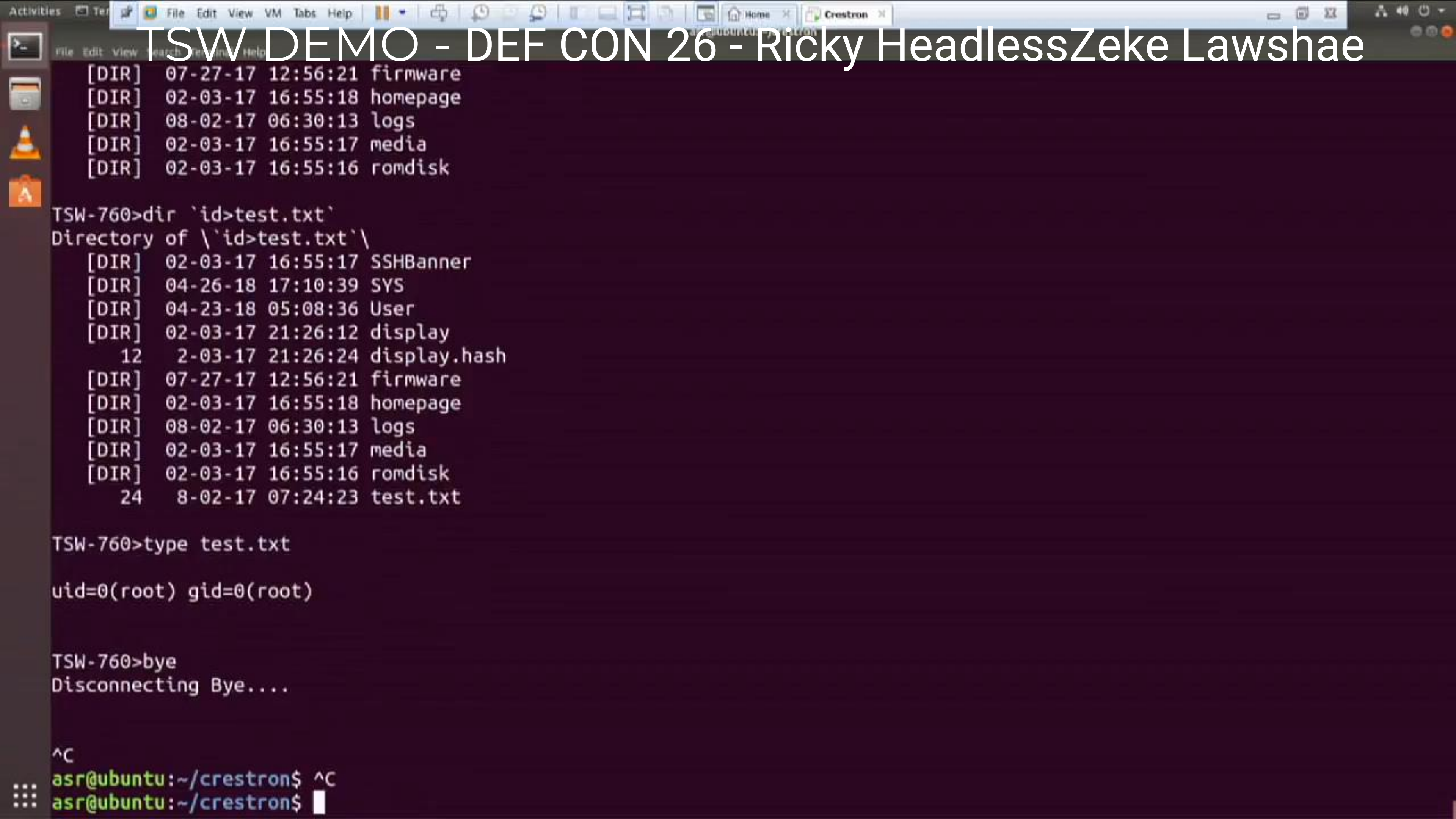
WHO Administrator Generate a report of the Ethernet consoles

Take Screenshot



```
TSW-1060>Generating a screen shot to /mnt/sdcard/ROMDISK/logs/ScreenShot.bmp
Screen width = 1280, height = 800
Raw image size is 4096000 bytes
Begin pixel grab and shuffle...Done!
BMP File Saved!


TSW-1060>
```

TSW DEMO - DEF CON 26 - Ricky HeadlessZeke Lawshae

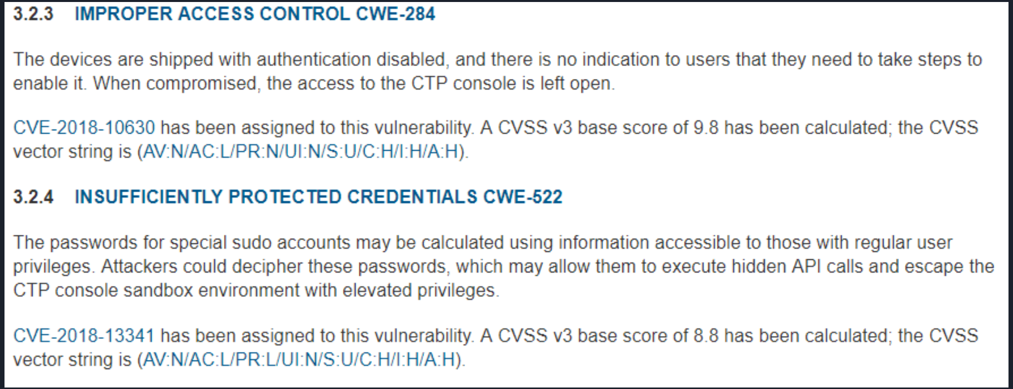

Activities
File Edit View VM Tabs Help
Home
Crestron
File Edit View Search Terminal Help

```
   [DIR]  07-27-17 12:56:21 firmware
   [DIR]  02-03-17 16:55:18 homepage
   [DIR]  08-02-17 06:30:13 logs
   [DIR]  02-03-17 16:55:17 media
   [DIR]  02-03-17 16:55:16 romdisk

TSW-760>dir `id>test.txt`
Directory of \`id>test.txt`\
   [DIR]  02-03-17 16:55:17 SSHBanner
   [DIR]  04-26-18 17:10:39 SYS
   [DIR]  04-23-18 05:08:36 User
   [DIR]  02-03-17 21:26:12 display
      12   2-03-17 21:26:24 display.hash
   [DIR]  07-27-17 12:56:21 firmware
   [DIR]  02-03-17 16:55:18 homepage
   [DIR]  08-02-17 06:30:13 logs
   [DIR]  02-03-17 16:55:17 media
   [DIR]  02-03-17 16:55:16 romdisk
      24   8-02-17 07:24:23 test.txt

TSW-760>type test.txt

uid=0(root) gid=0(root)


TSW-760>bye
Disconnecting Bye....


^C
asr@ubuntu:~/crestron$ ^C
asr@ubuntu:~/crestron$ 
```

Crestron MC3 Controller

Vulnerabilities

- Authentication disabled by default
- Can decipher super user passwords
- Firmware older than 1.502.0047.001



3.2.3 IMPROPER ACCESS CONTROL CWE-284

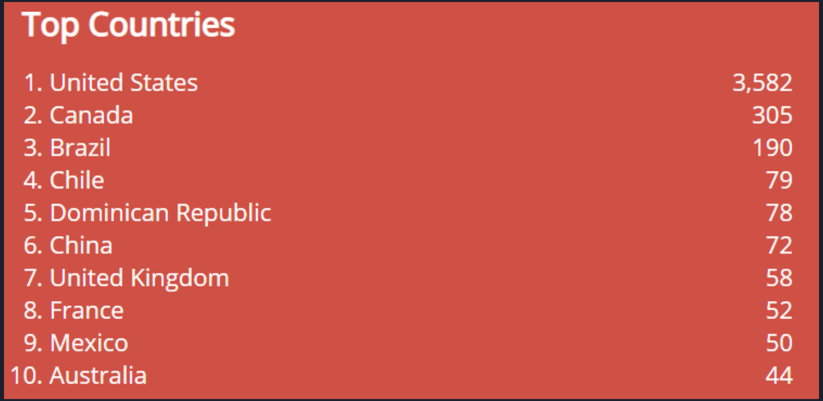
The devices are shipped with authentication disabled, and there is no indication to users that they need to take steps to enable it. When compromised, the access to the CTP console is left open.

CVE-2018-10630 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.2.4 INSUFFICIENTLY PROTECTED CREDENTIALS CWE-522

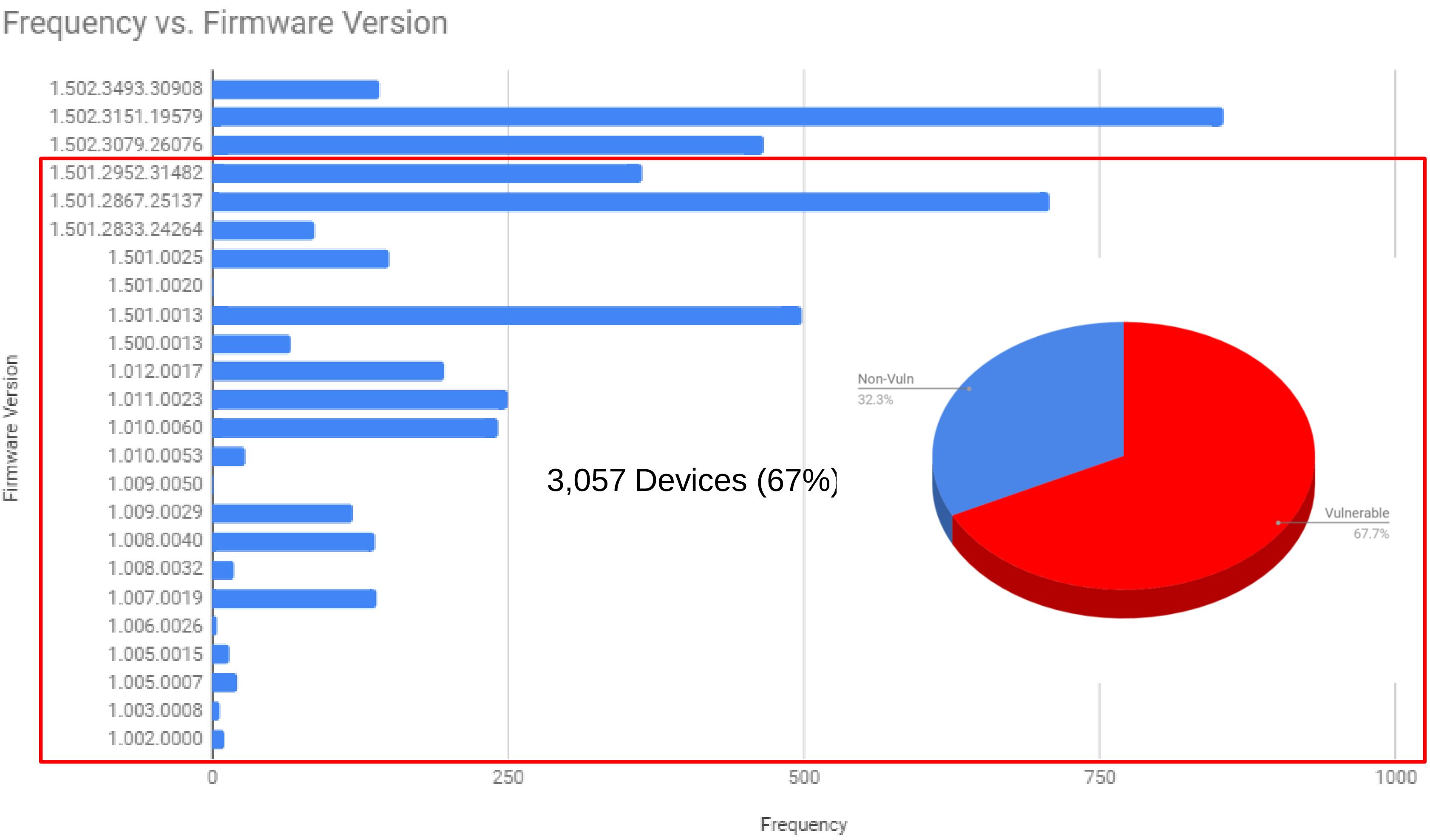
The passwords for special sudo accounts may be calculated using information accessible to those with regular user privileges. Attackers could decipher these passwords, which may allow them to execute hidden API calls and escape the CTP console sandbox environment with elevated privileges.

CVE-2018-13341 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).



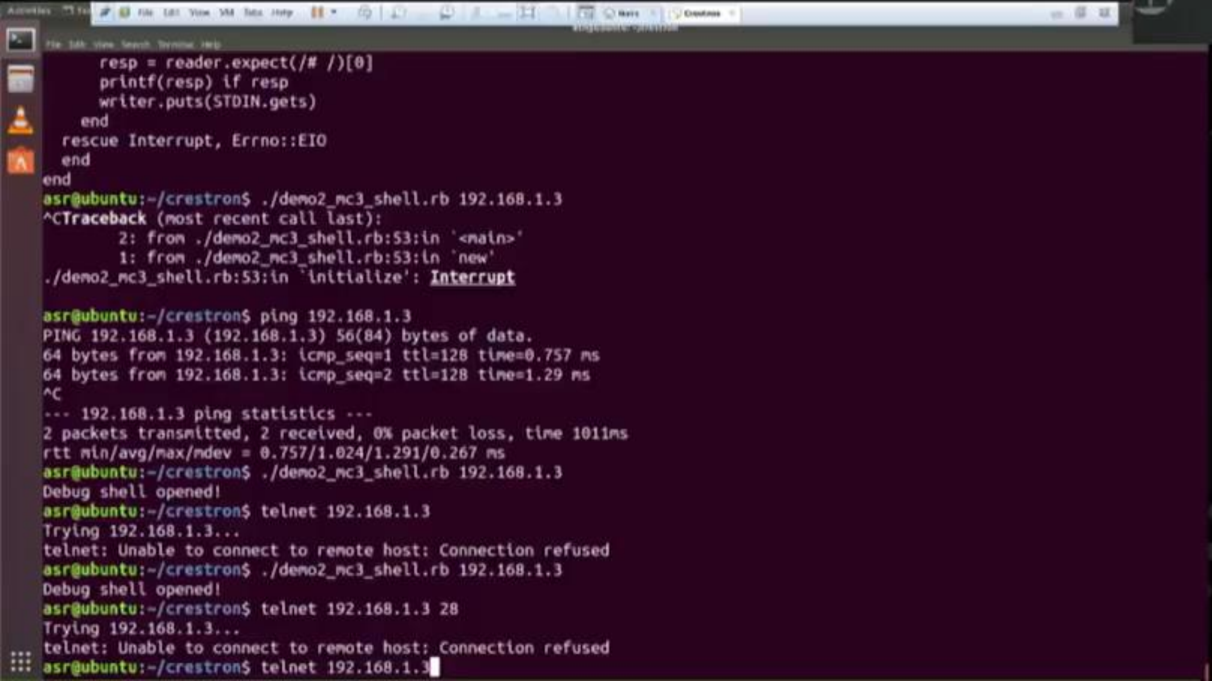
Top Countries

1. United States	3,582
2. Canada	305
3. Brazil	190
4. Chile	79
5. Dominican Republic	78
6. China	72
7. United Kingdom	58
8. France	52
9. Mexico	50
10. Australia	44



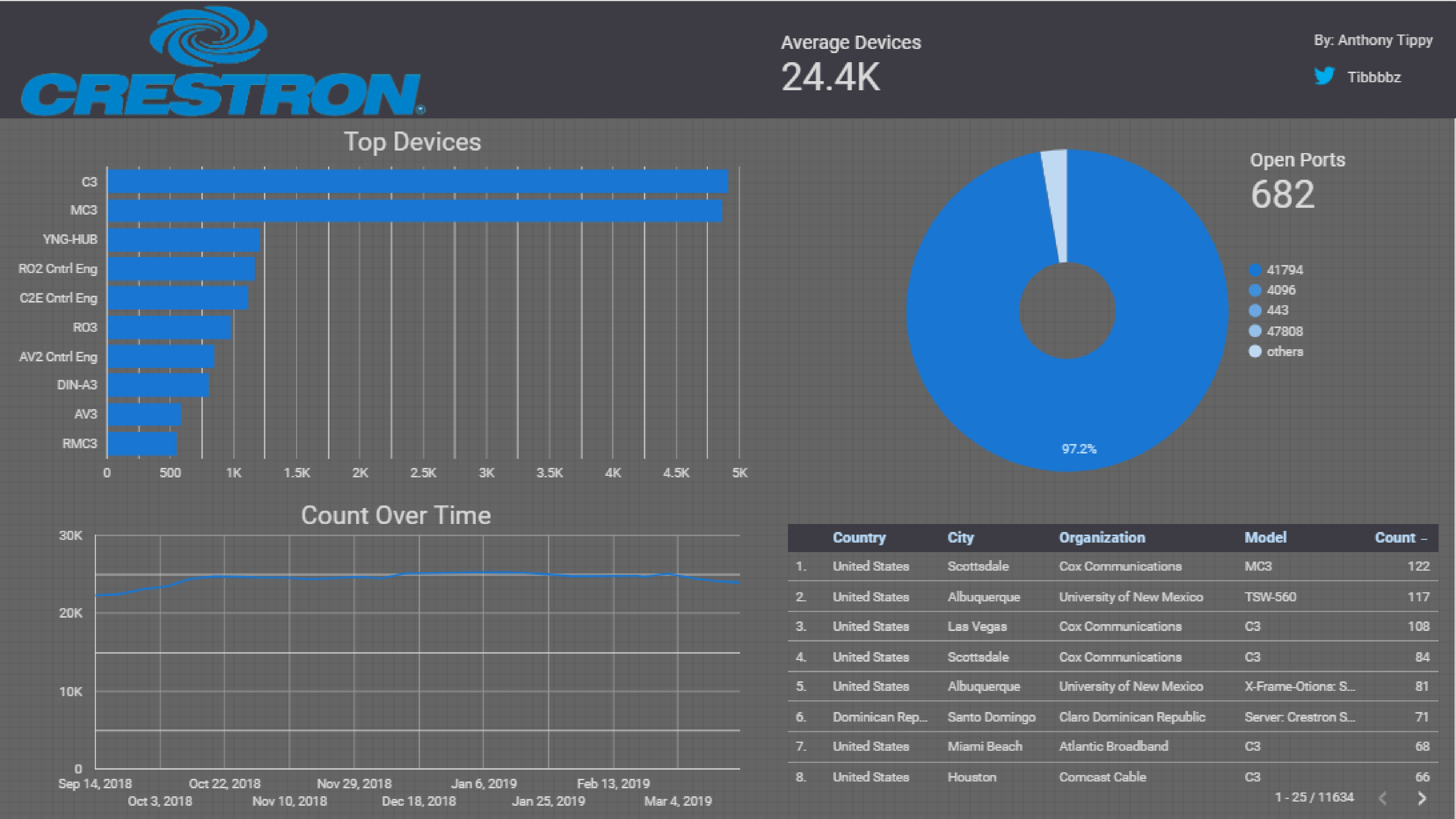
3,057 Devices (67%)

MC3 Demo- DEF CON 26 - Ricky 'HeadlessZeke' Lawshae



```
      resp = reader.expect(/# /)[0]
      printf(resp) if resp
      writer.puts(STDIN.gets)
    end
  rescue Interrupt, Errno::EIO
  end
end
asr@ubuntu:~/crestron$ ./demo2_mc3_shell.rb 192.168.1.3
^CTraceback (most recent call last):
        2: from ./demo2_mc3_shell.rb:53:in `<main>'
        1: from ./demo2_mc3_shell.rb:53:in `new'
./demo2_mc3_shell.rb:53:in `initialize': Interrupt

asr@ubuntu:~/crestron$ ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=128 time=0.757 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=128 time=1.29 ms
^C
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1011ms
rtt min/avg/max/mdev = 0.757/1.024/1.291/0.267 ms
asr@ubuntu:~/crestron$ ./demo2_mc3_shell.rb 192.168.1.3
Debug shell opened!
asr@ubuntu:~/crestron$ telnet 192.168.1.3
Trying 192.168.1.3...
telnet: Unable to connect to remote host: Connection refused
asr@ubuntu:~/crestron$ ./demo2_mc3_shell.rb 192.168.1.3
Debug shell opened!
asr@ubuntu:~/crestron$ telnet 192.168.1.3 28
Trying 192.168.1.3...
telnet: Unable to connect to remote host: Connection refused
asr@ubuntu:~/crestron$ telnet 192.168.1.3
```

AUGUST 9-12, 2018
LAS VEGAS



Average Devices

24.4K

By: Anthony Tippy

Tibbbbz

Top Devices

Open Ports

682

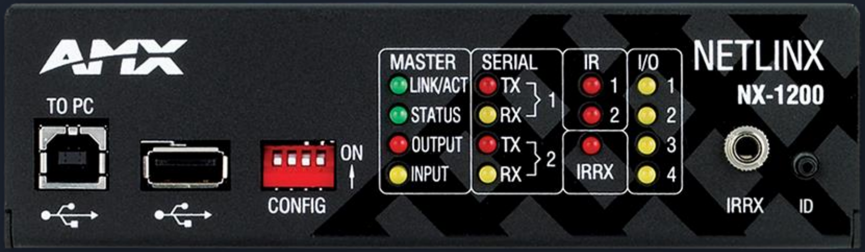
Count Over Time

	Country	City	Organization	Model	Count ↓
1.	United States	Scottsdale	Cox Communications	MC3	122
2.	United States	Albuquerque	University of New Mexico	TSW-560	117
3.	United States	Las Vegas	Cox Communications	C3	108
4.	United States	Scottsdale	Cox Communications	C3	84
5.	United States	Albuquerque	University of New Mexico	X-Frame-Otions: S...	81
6.	Dominican Rep...	Santo Domingo	Claro Dominican Republic	Server: Crestron S...	71
7.	United States	Miami Beach	Atlantic Broadband	C3	68
8.	United States	Houston	Comcast Cable	C3	66

1 - 25 / 11634 < >

AMX Systems

NetLinx Intergrated Controller
AMX


AMX
TO PC
CONFIG
ON
MASTER
LINK/ACT
STATUS
OUTPUT
INPUT
SERIAL
TX
RX
1
TX
RX
2
IR
1
2
IRRX
I/O
1
2
3
4
NETLINX
NX-1200
IRRX
ID

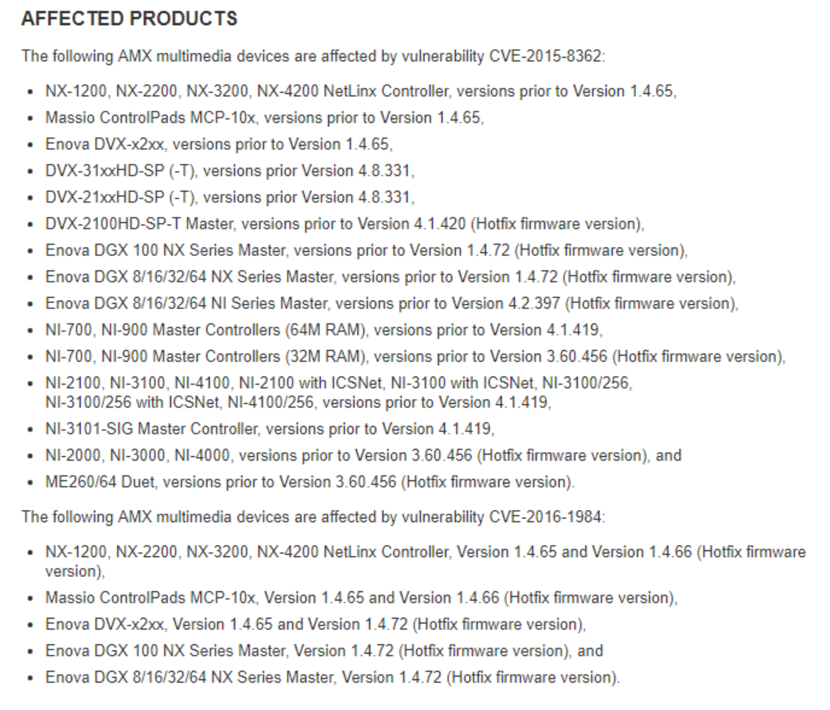
ABC Company
VIDEO CONFERENCE

Past Vulnerabilities

CVE-2015-8362

- Back Door account access
- “The usernames *"1MB@tMaN"* and *“BlackWidow"* were hard-coded in the firmware and allow for remote login in debug mode, granting the attacker access to tools not provided to administrators such as packet sniffing.”

CVE-2015-8362- BackDoors



AFFECTED PRODUCTS

The following AMX multimedia devices are affected by vulnerability CVE-2015-8362:

- NX-1200, NX-2200, NX-3200, NX-4200 NetLinx Controller, versions prior to Version 1.4.65,
- Massio ControlPads MCP-10x, versions prior to Version 1.4.65,
- Enova DVX-x2xx, versions prior to Version 1.4.65,
- DVX-31xxHD-SP (-T), versions prior Version 4.8.331,
- DVX-21xxHD-SP (-T), versions prior Version 4.8.331,
- DVX-2100HD-SP-T Master, versions prior to Version 4.1.420 (Hotfix firmware version),
- Enova DGX 100 NX Series Master, versions prior to Version 1.4.72 (Hotfix firmware version),
- Enova DGX 8/16/32/64 NX Series Master, versions prior to Version 1.4.72 (Hotfix firmware version),
- Enova DGX 8/16/32/64 NI Series Master, versions prior to Version 4.2.397 (Hotfix firmware version),
- NI-700, NI-900 Master Controllers (64M RAM), versions prior to Version 4.1.419,
- NI-700, NI-900 Master Controllers (32M RAM), versions prior to Version 3.60.456 (Hotfix firmware version),
- NI-2100, NI-3100, NI-4100, NI-2100 with ICSNet, NI-3100 with ICSNet, NI-3100/256, NI-3100/256 with ICSNet, NI-4100/256, versions prior to Version 4.1.419,
- NI-3101-SIG Master Controller, versions prior to Version 4.1.419,
- NI-2000, NI-3000, NI-4000, versions prior to Version 3.60.456 (Hotfix firmware version), and
- ME260/64 Duet, versions prior to Version 3.60.456 (Hotfix firmware version).

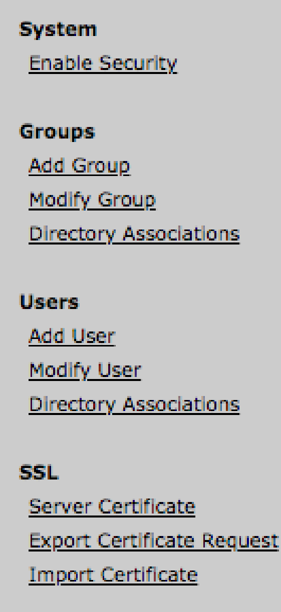
The following AMX multimedia devices are affected by vulnerability CVE-2016-1984:

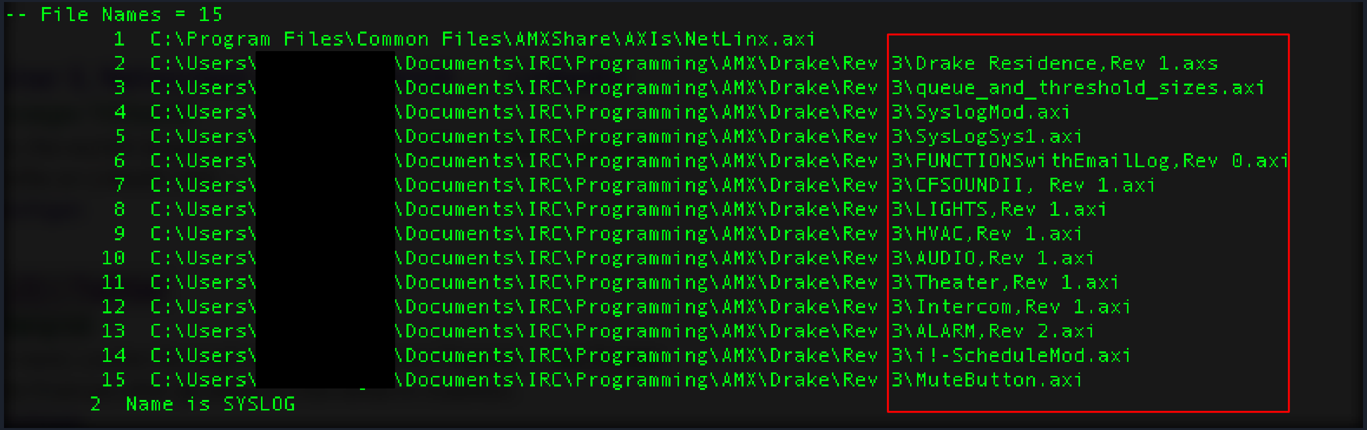
- NX-1200, NX-2200, NX-3200, NX-4200 NetLinx Controller, Version 1.4.65 and Version 1.4.66 (Hotfix firmware version),
- Massio ControlPads MCP-10x, Version 1.4.65 and Version 1.4.66 (Hotfix firmware version),
- Enova DVX-x2xx, Version 1.4.65 and Version 1.4.72 (Hotfix firmware version),
- Enova DGX 100 NX Series Master, Version 1.4.72 (Hotfix firmware version), and
- Enova DGX 8/16/32/64 NX Series Master, Version 1.4.72 (Hotfix firmware version).

- elevated privileges to configure user interfaces, change device settings, upload files, and download file
- Break all the things!

CVE-2015-8362- Hardcoded password

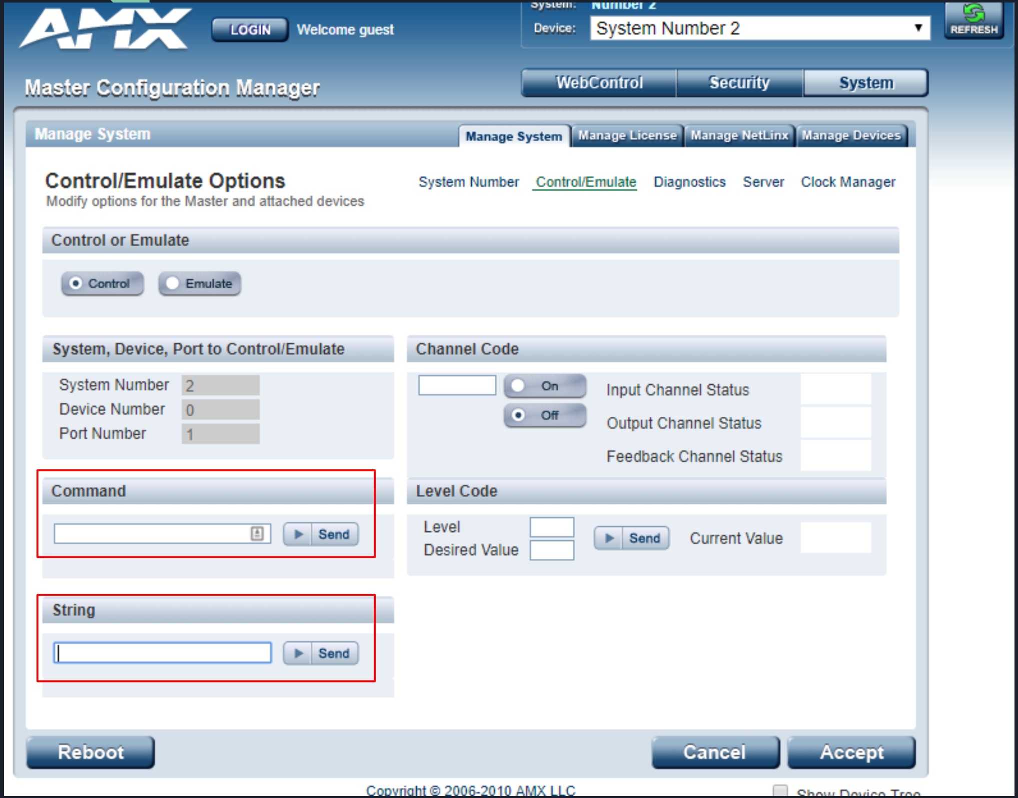
- Fully unauthenticated
- Web Interface pretty buggy
- Appears to be a “Smart Home”





```
-- File Names = 15
         1  C:\Program Files\Common Files\AMXShare\AXIs\NetLinx.axi
         2  C:\Users\[redacted]\Documents\IRC\Programming\AMX\Drake\Rev 3\Drake Residence,Rev 1.axs
         3  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\queue_and_threshold_sizes.axi
         4  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\SyslogMod.axi
         5  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\SysLogSys1.axi
         6  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\FUNCTIONSwithEmailLog,Rev 0.axi
         7  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\CFSOUNDII, Rev 1.axi
         8  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\LIGHTS,Rev 1.axi
         9  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\HVAC,Rev 1.axi
        10  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\AUDIO,Rev 1.axi
        11  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\Theater,Rev 1.axi
        12  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\Intercom,Rev 1.axi
        13  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\ALARM,Rev 2.axi
        14  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\i!-ScheduleMod.axi
        15  C:\Users\\Documents\IRC\Programming\AMX\Drake\Rev 3\MuteButton.axi
       2  Name is SYSLOG
```

AMX Web Control- Unauthenticated

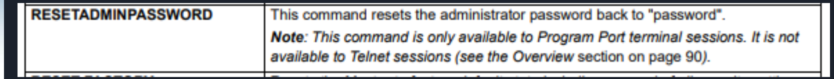


Device: System Number 2

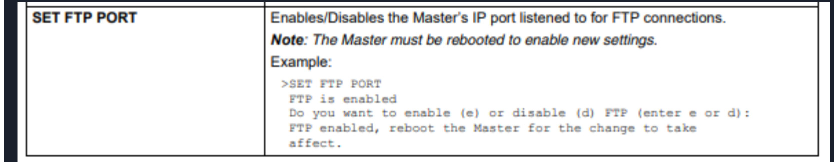
● Control ○ Emulate

System Number 2
Device Number 0
Port Number 1

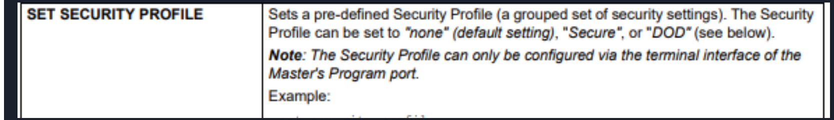
○ On ● Off



RESETADMINPASSWORD	This command resets the administrator password back to "password". ***Note****: This command is only available to Program Port terminal sessions. It is not available to Telnet sessions (see the Overview section on page 90).*

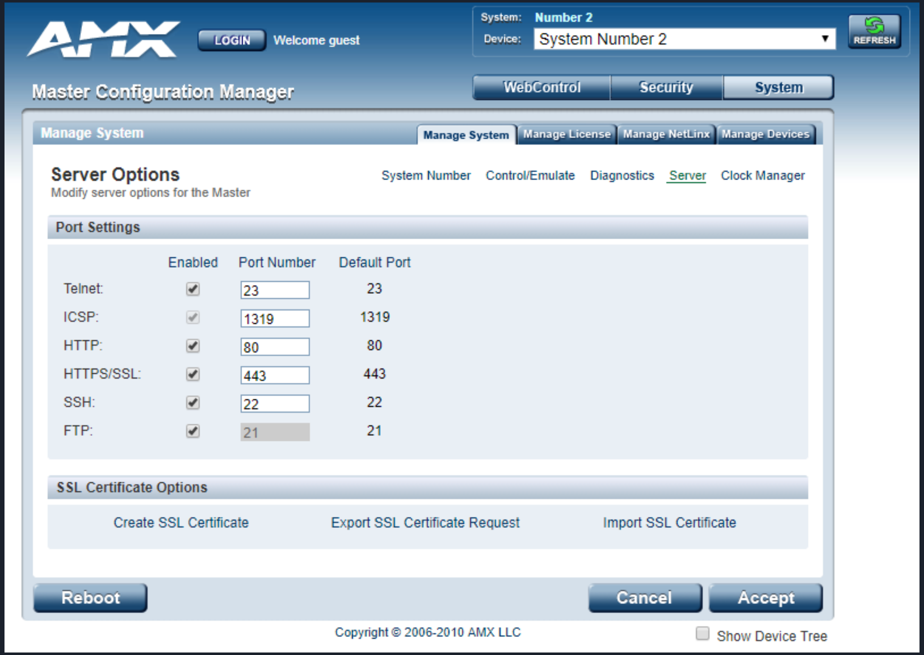


SET FTP PORT	Enables/Disables the Master's IP port listened to for FTP connections.
	Note*: The Master must be rebooted to enable new settings.*
	Example:
	`>SET FTP PORT`
	`FTP is enabled`
	`Do you want to enable (e) or disable (d) FTP (enter e or d):`
	`FTP enabled, reboot the Master for the change to take affect.`



SET SECURITY PROFILE	Sets a pre-defined Security Profile (a grouped set of security settings). The Security Profile can be set to *"none" (default setting)*, *"Secure"*, or *"DOD"* (see below). ***Note****: The Security Profile can only be configured via the terminal interface of the Master's Program port.* Example:

Change all the things!



System: Number 2

Device: System Number 2

Manage System

Server Options

Modify server options for the Master

Port Settings

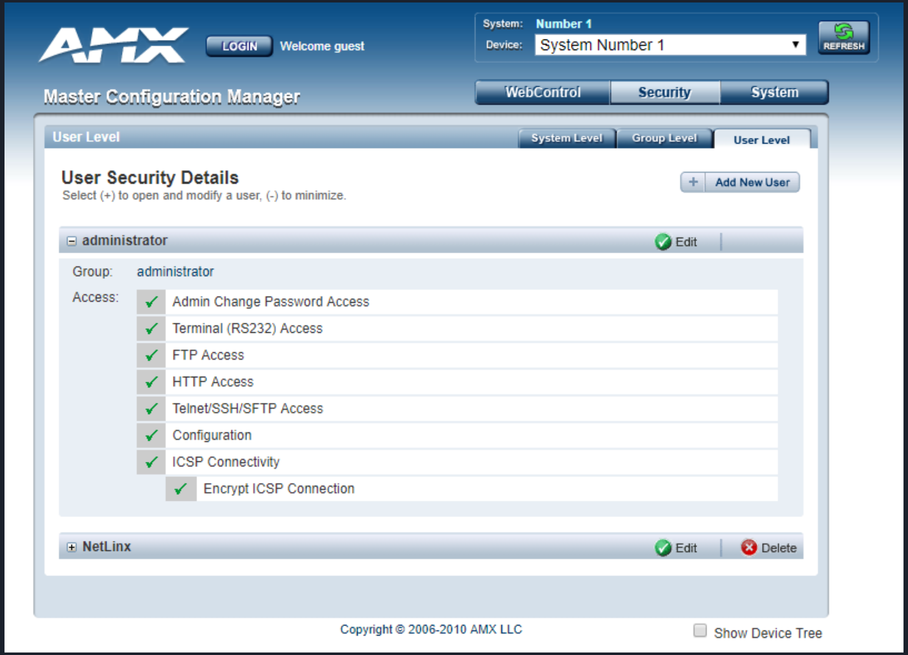
	Enabled	Port Number	Default Port
Telnet:	☑	23	23
ICSP:	☑	1319	1319
HTTP:	☑	80	80
HTTPS/SSL:	☑	443	443
SSH:	☑	22	22
FTP:	☑	21	21

SSL Certificate Options

Create SSL Certificate Export SSL Certificate Request Import SSL Certificate

□ Show Device Tree

Copyright © 2006-2010 AMX LLC



System: Number 1

Device: System Number 1

User Level

User Security Details

Select (+) to open and modify a user, (-) to minimize.

⊟ administrator

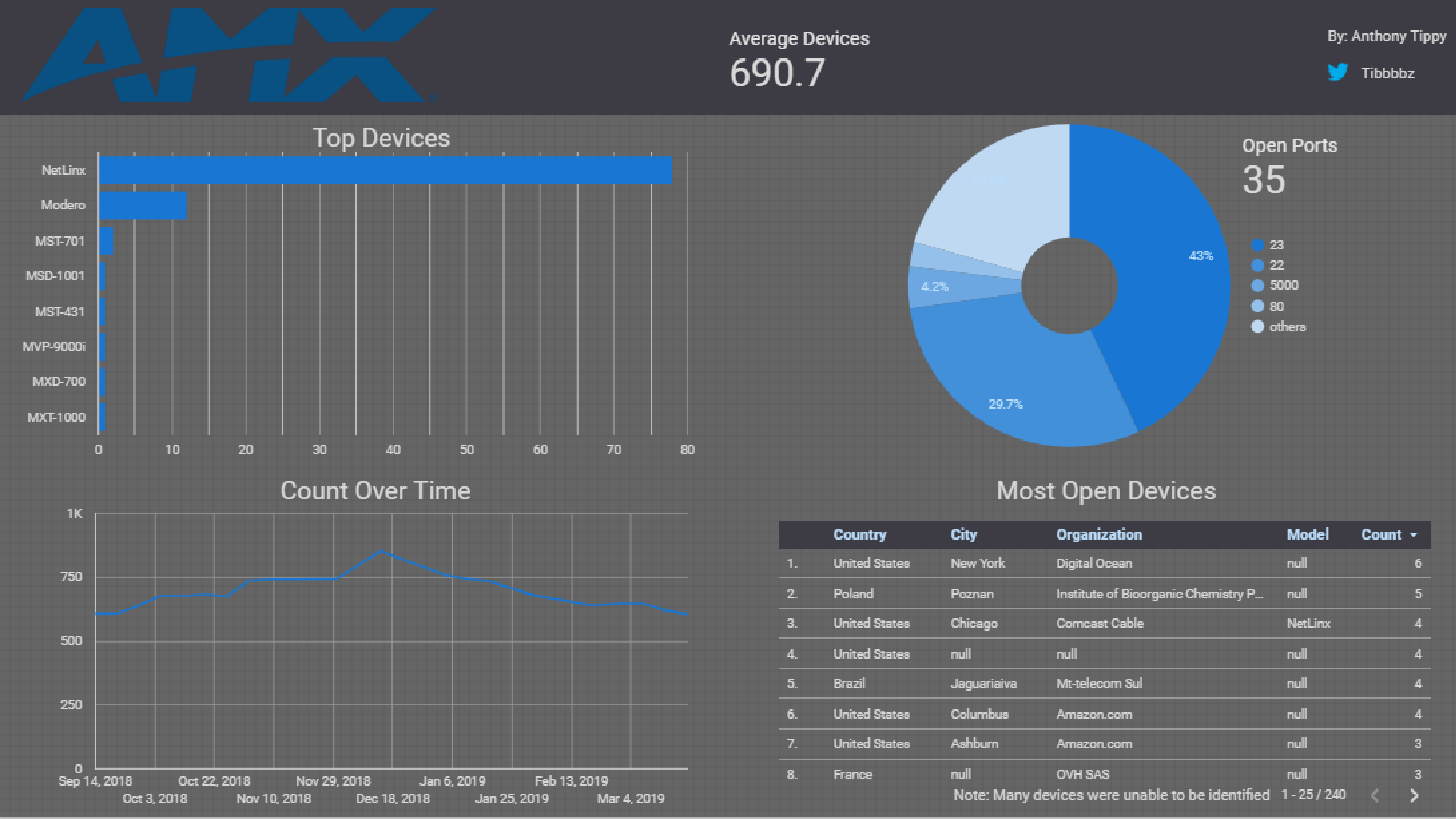
Group: administrator

Access:
- ✓ Admin Change Password Access
- ✓ Terminal (RS232) Access
- ✓ FTP Access
- ✓ HTTP Access
- ✓ Telnet/SSH/SFTP Access
- ✓ Configuration
- ✓ ICSP Connectivity
  - ✓ Encrypt ICSP Connection

⊞ NetLinx

Copyright © 2006-2010 AMX LLC

□ Show Device Tree



Average Devices

690.7

By: Anthony Tippy

Tibbbbz

Top Devices

Open Ports

35

Count Over Time

Most Open Devices

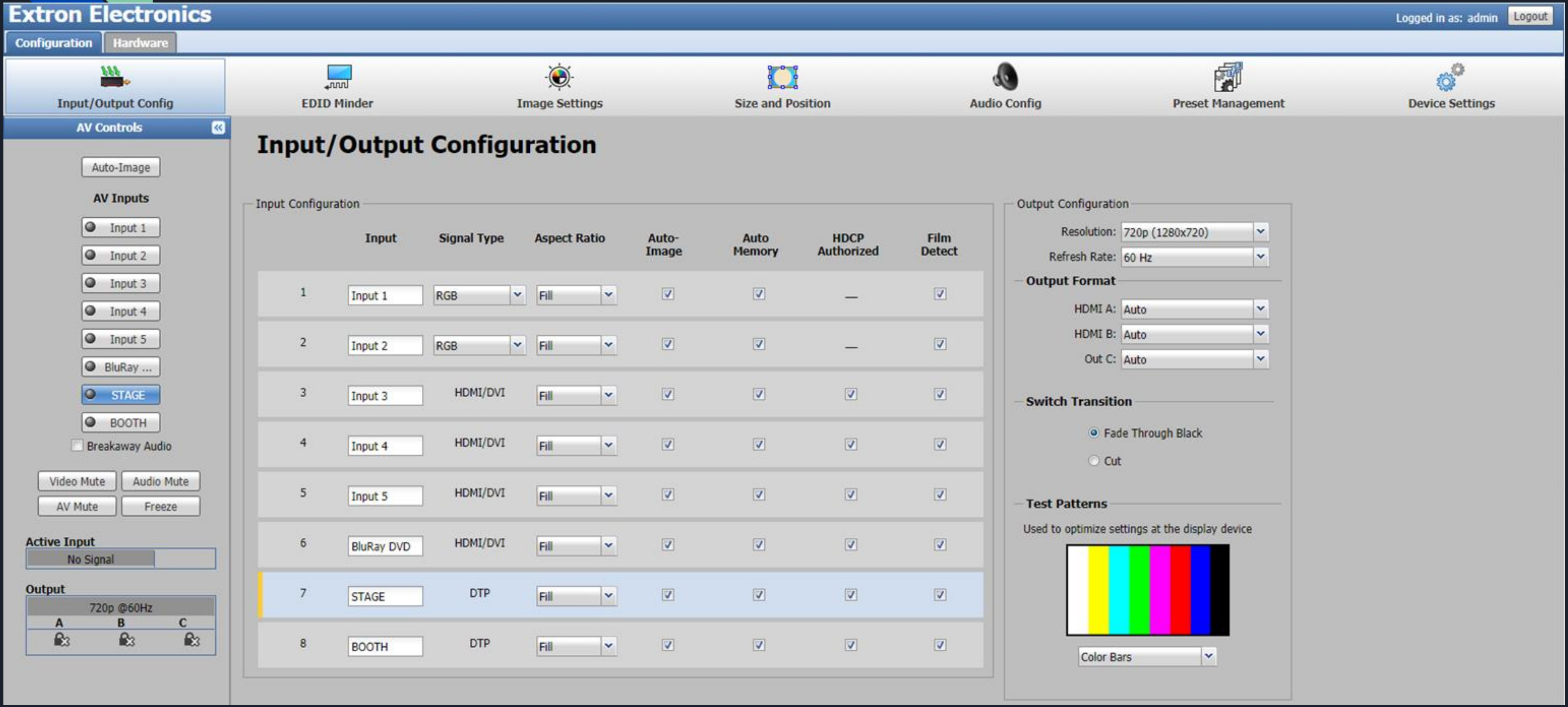
	Country	City	Organization	Model	Count ▾
1.	United States	New York	Digital Ocean	null	6
2.	Poland	Poznan	Institute of Bioorganic Chemistry P...	null	5
3.	United States	Chicago	Comcast Cable	NetLinx	4
4.	United States	null	null	null	4
5.	Brazil	Jaguariaiva	Mt-telecom Sul	null	4
6.	United States	Columbus	Amazon.com	null	4
7.	United States	Ashburn	Amazon.com	null	3
8.	France	null	OVH SAS	null	3

Note: Many devices were unable to be identified

Misc Hardware Devices

Extron IN1608 Switcher

- No authentication Required
- Logs in as Admin
- Extron IN1608 SA- 8 Input switcher/ scaler



Active Input: No Signal

Output: 720p @60Hz

A	B	C

Input/Output Configuration

Input Configuration

	Input	Signal Type	Aspect Ratio	Auto-Image	Auto Memory	HDCP Authorized	Film Detect
1	Input 1	RGB	Fill	☑	☑	—	☑
2	Input 2	RGB	Fill	☑	☑	—	☑
3	Input 3	HDMI/DVI	Fill	☑	☑	☑	☑
4	Input 4	HDMI/DVI	Fill	☑	☑	☑	☑
5	Input 5	HDMI/DVI	Fill	☑	☑	☑	☑
6	BluRay DVD	HDMI/DVI	Fill	☑	☑	☑	☑
7	STAGE	DTP	Fill	☑	☑	☑	☑
8	BOOTH	DTP	Fill	☑	☑	☑	☑

Output Configuration

Resolution: 720p (1280x720)

Refresh Rate: 60 Hz

Output Format

HDMI A: Auto

HDMI B: Auto

Out C: Auto

Switch Transition

● Fade Through Black

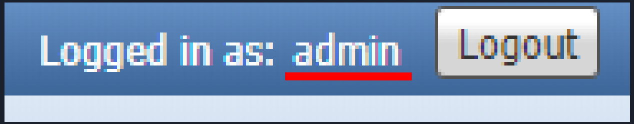
○ Cut

Test Patterns

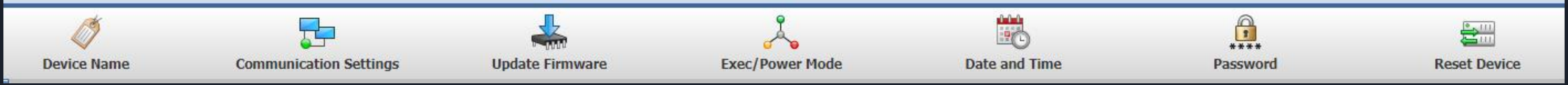
Used to optimize settings at the display device

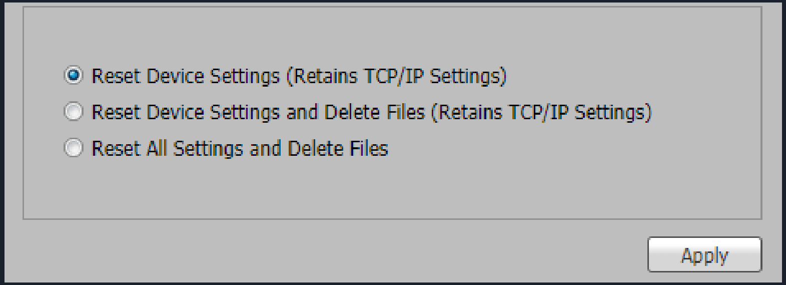
Color Bars

Oh boy...



Logged in as: admin

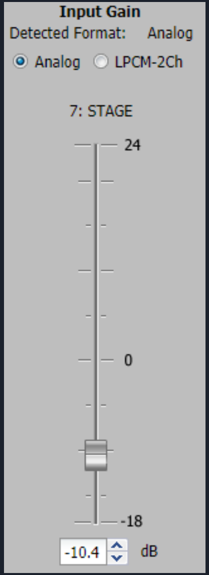




● Reset Device Settings (Retains TCP/IP Settings)

○ Reset Device Settings and Delete Files (Retains TCP/IP Settings)

○ Reset All Settings and Delete Files



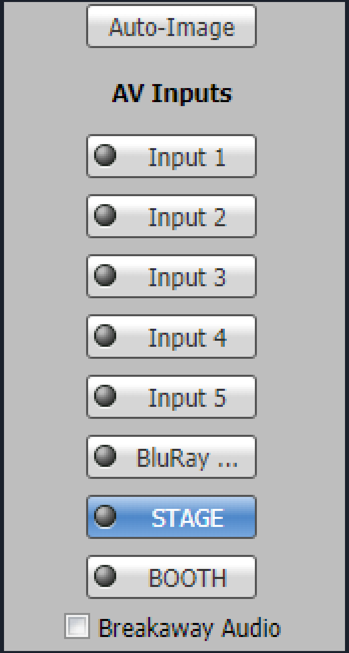
Input Gain

Detected Format: Analog

● Analog ○ LPCM-2Ch

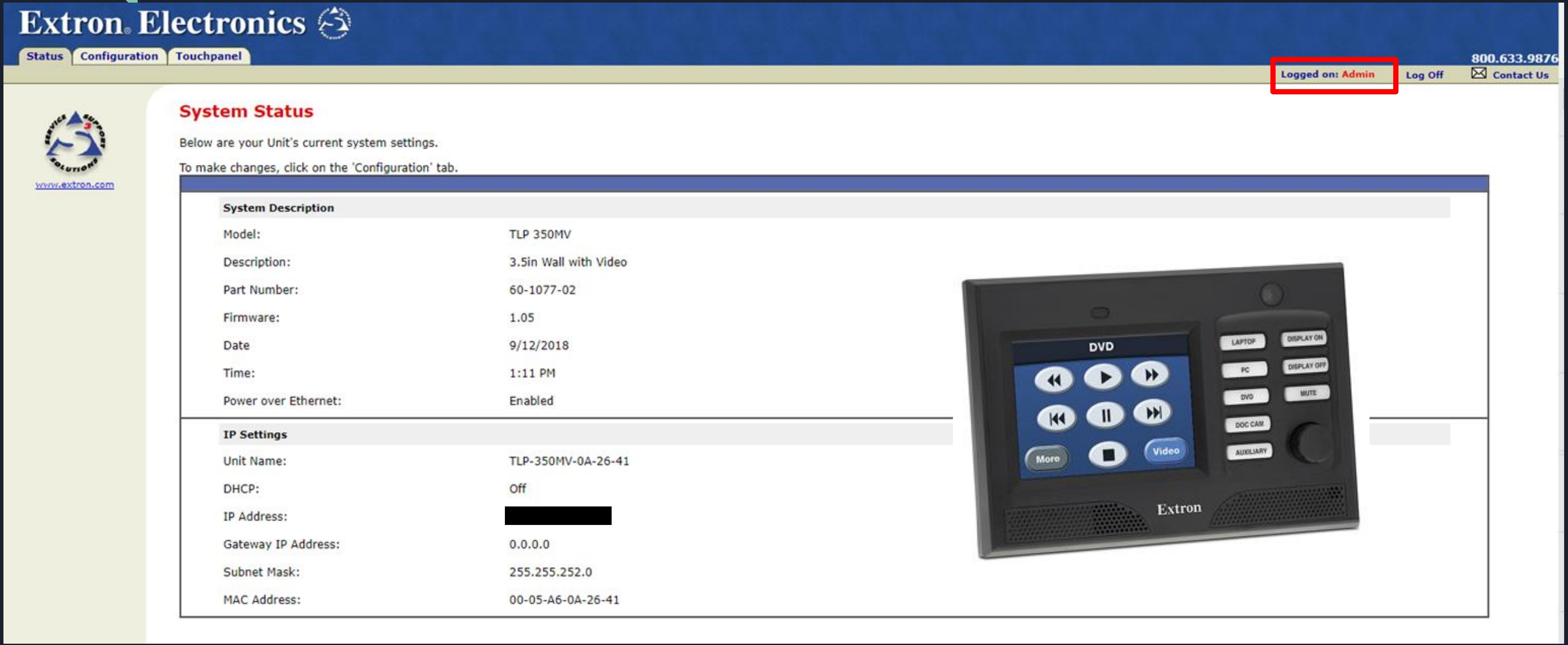
7: STAGE

-10.4 dB



□ Breakaway Audio

Extron Controllers- Extron TLP 350MV

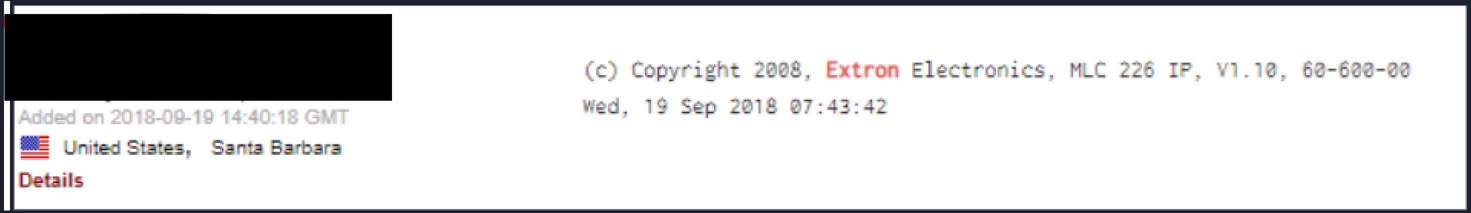


System Status

Below are your Unit's current system settings.

To make changes, click on the 'Configuration' tab.

System Description	
Model:	TLP 350MV
Description:	3.5in Wall with Video
Part Number:	60-1077-02
Firmware:	1.05
Date	9/12/2018
Time:	1:11 PM
Power over Ethernet:	Enabled
IP Settings	
Unit Name:	TLP-350MV-0A-26-41
DHCP:	Off
IP Address:	[redacted]
Gateway IP Address:	0.0.0.0
Subnet Mask:	255.255.252.0
MAC Address:	00-05-A6-0A-26-41



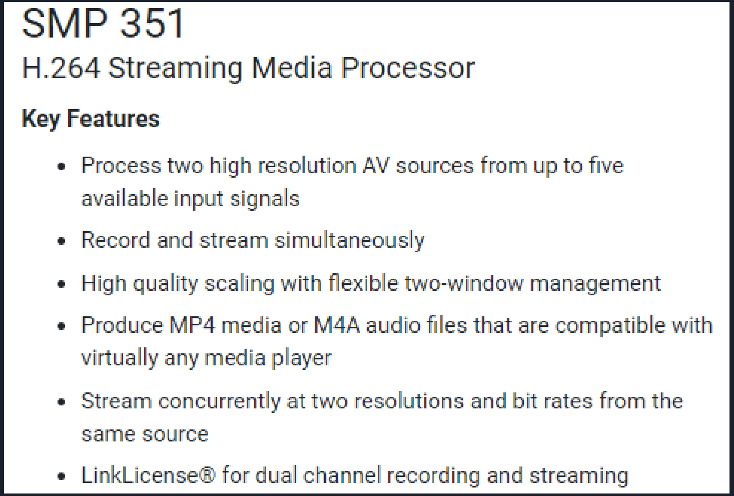
[redacted]

Added on 2018-09-19 14:40:18 GMT

🇺🇸 United States, Santa Barbara

Details

```
(c) Copyright 2008, Extron Electronics, MLC 226 IP, V1.10, 60-600-00
Wed, 19 Sep 2018 07:43:42
```

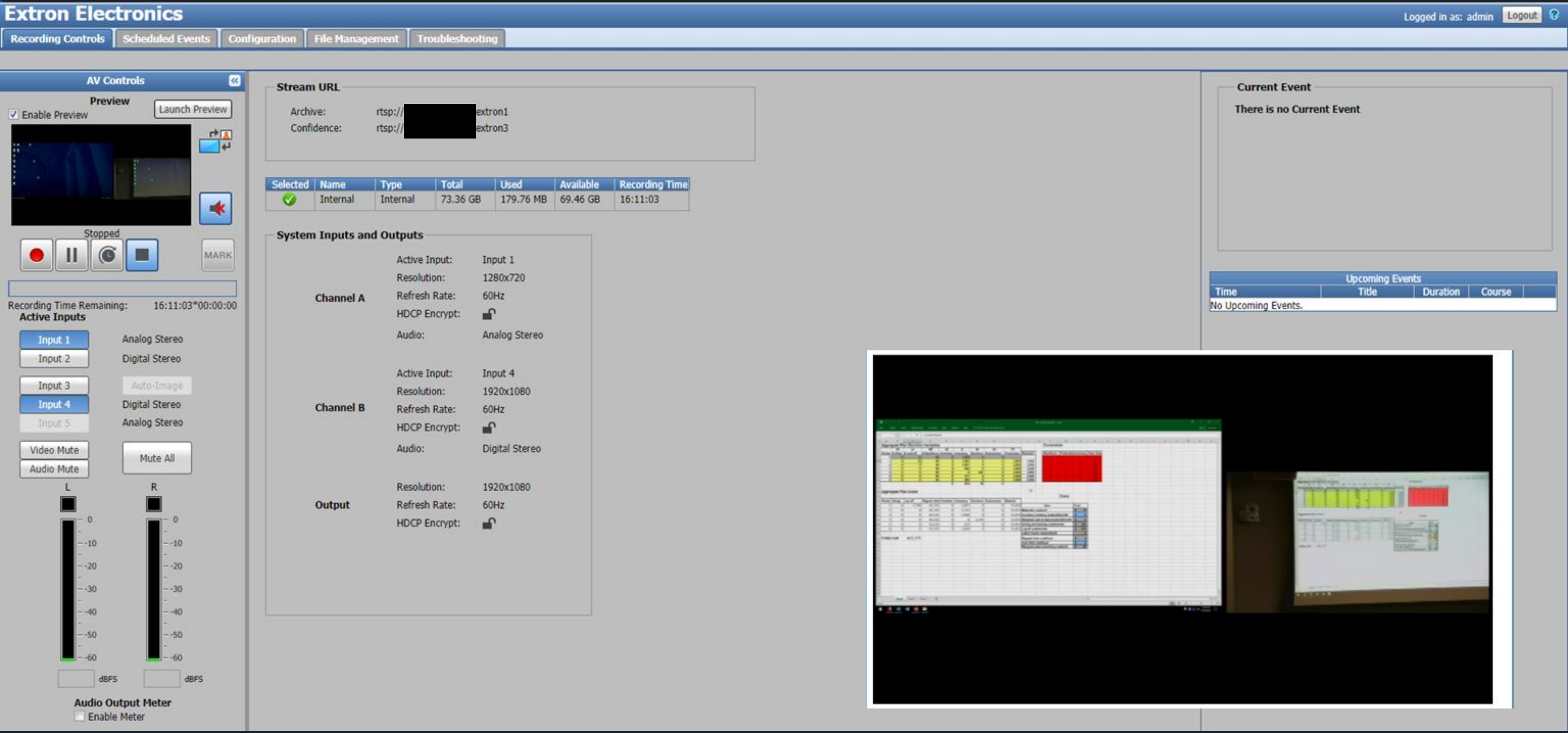


SMP 351

H.264 Streaming Media Processor

Key Features

- Process two high resolution AV sources from up to five available input signals
- Record and stream simultaneously
- High quality scaling with flexible two-window management
- Produce MP4 media or M4A audio files that are compatible with virtually any media player
- Stream concurrently at two resolutions and bit rates from the same source
- LinkLicense® for dual channel recording and streaming



☑ Enable Preview

Stopped

Recording Time Remaining: 16:11:03*00:00:00

Active Inputs

Input 1	Analog Stereo
Input 2	Digital Stereo
Input 3	Auto-Image
Input 4	Digital Stereo
Input 5	Analog Stereo

Audio Output Meter

□ Enable Meter

Stream URL

Archive: rtsp://[redacted]extron1
Confidence: rtsp://[redacted]extron3

Selected	Name	Type	Total	Used	Available	Recording Time
✓	Internal	Internal	73.36 GB	179.76 MB	69.46 GB	16:11:03

System Inputs and Outputs

Channel A
Active Input: Input 1
Resolution: 1280x720
Refresh Rate: 60Hz
HDCP Encrypt: 🔓
Audio: Analog Stereo

Channel B
Active Input: Input 4
Resolution: 1920x1080
Refresh Rate: 60Hz
HDCP Encrypt: 🔓
Audio: Digital Stereo

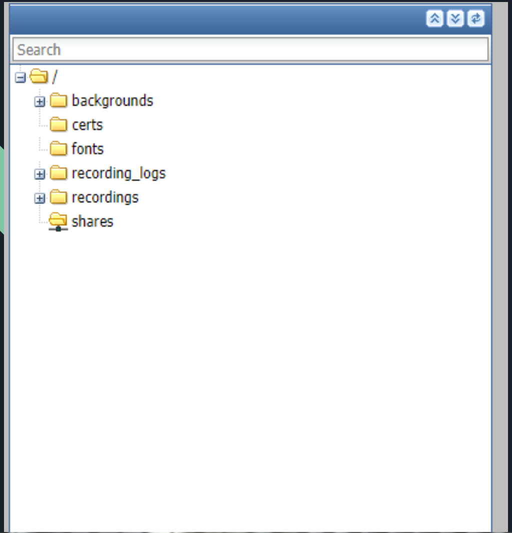
Output
Resolution: 1920x1080
Refresh Rate: 60Hz
HDCP Encrypt: 🔓

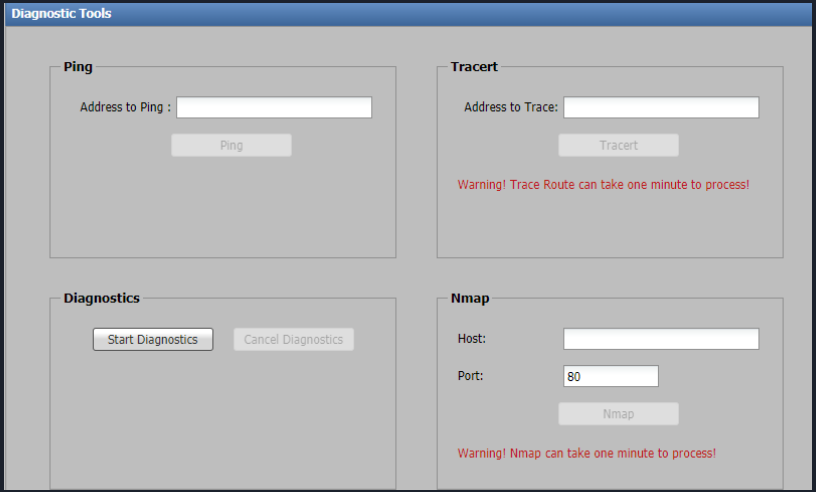
Current Event

There is no Current Event

Upcoming Events

Time	Title	Duration	Course
No Upcoming Events.			





Diagnostic Tools

Ping

Address to Ping :

Tracert

Address to Trace:

Warning! Trace Route can take one minute to process!

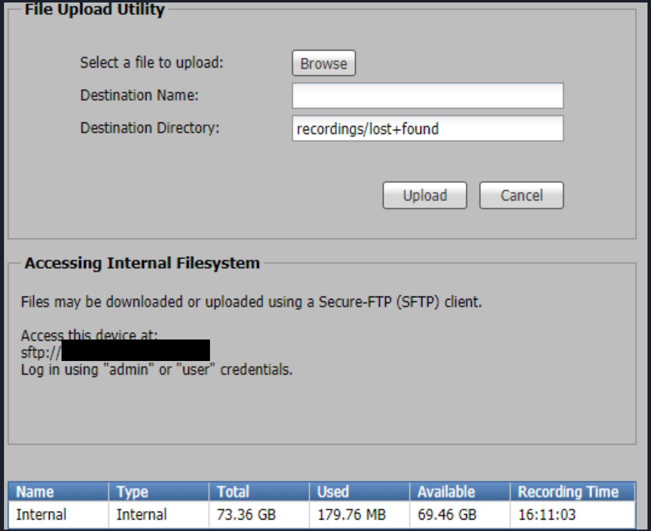
Diagnostics

Nmap

Host:

Port: 80

Warning! Nmap can take one minute to process!



File Upload Utility

Select a file to upload:

Destination Name:

Destination Directory: recordings/lost+found

Accessing Internal Filesystem

Files may be downloaded or uploaded using a Secure-FTP (SFTP) client.

Access this device at:
sftp://[redacted]
Log in using "admin" or "user" credentials.

Name	Type	Total	Used	Available	Recording Time
Internal	Internal	73.36 GB	179.76 MB	69.46 GB	16:11:03

Extron

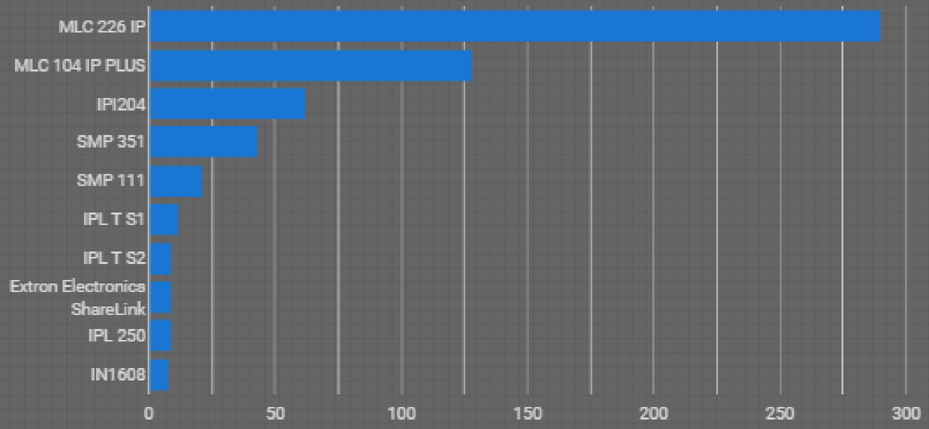
Average Devices

676.5

By: Anthony Tippy

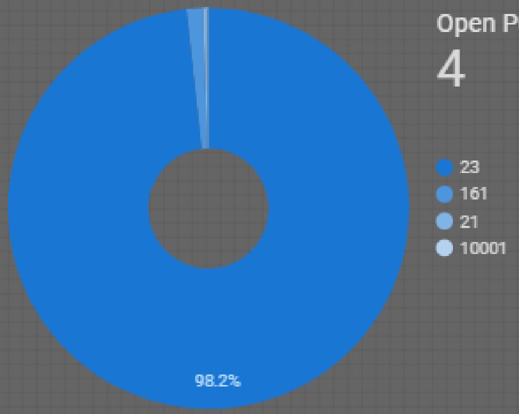
Tibbbbz

Top Devices

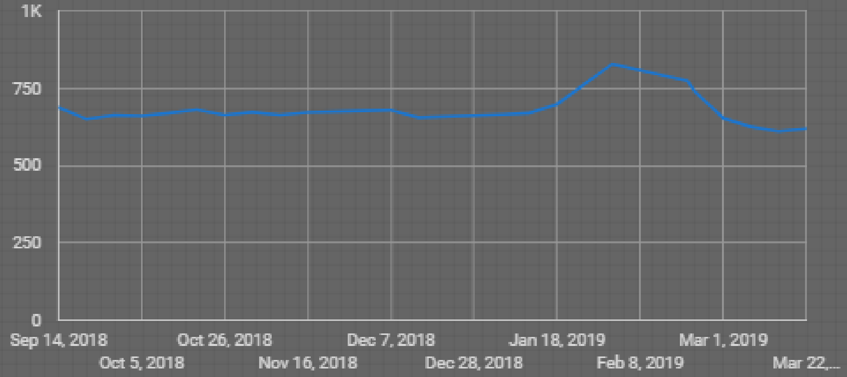


Open Ports

4



Count Over Time

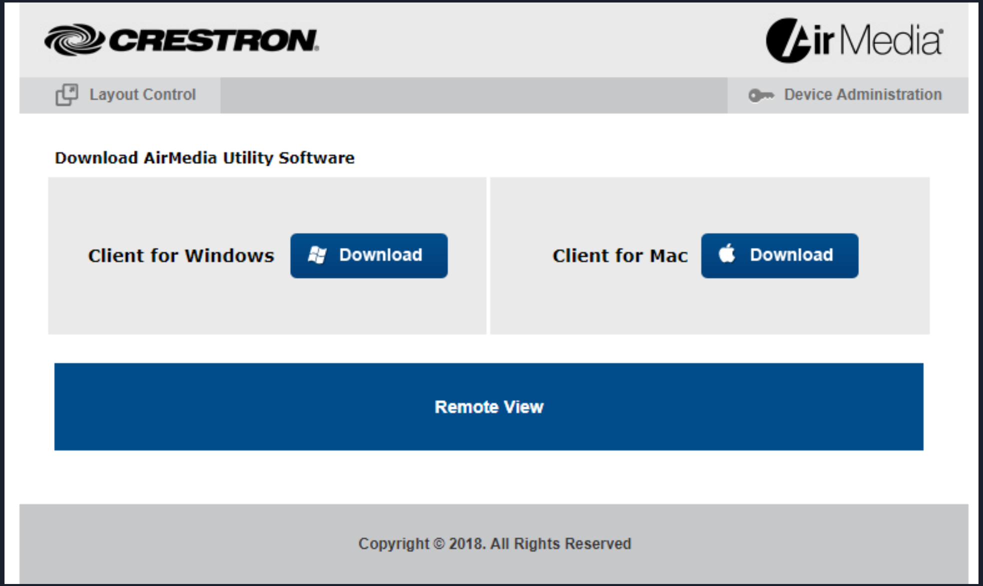


Most Open Devices

	Country	City	Organization	Model	Count ▾
1.	United States	Santa Barbara	University of California, Santa...	MLC 226 IP	76
2.	United States	Philadelphia	University of Pennsylvania	IPI204	60
3.	Taiwan	null	Taiwan Academic Network (T...	MLC 226 IP	53
4.	United States	Philadelphia	University of Pennsylvania	MLC 226 IP	47
5.	Germany	Landau	University of Koblenz-Landau	MLC 226 IP	28
6.	United States	Cambridge	Massachusetts Institute of T...	MLC 226 IP	25
7.	United States	Baltimore	University of Maryland Baltim...	MLC 104 IP PL...	24

1 - 25 / 163 ‹ ›

Crestron Air Media



CRESTRON AirMedia

Layout Control | Device Administration

Download AirMedia Utility Software

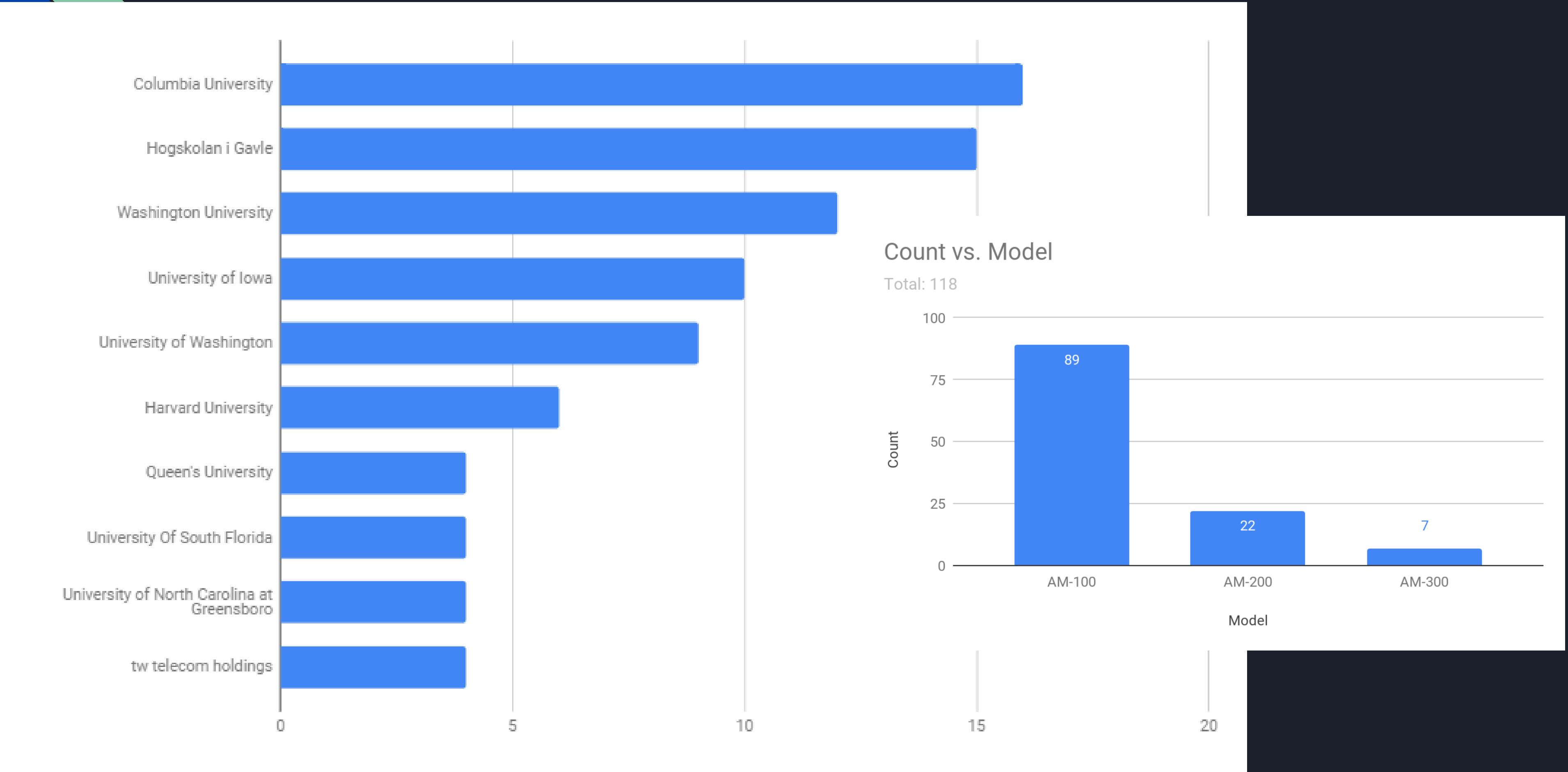
Client for Windows [Download]

Client for Mac [Download]

[Remote View]

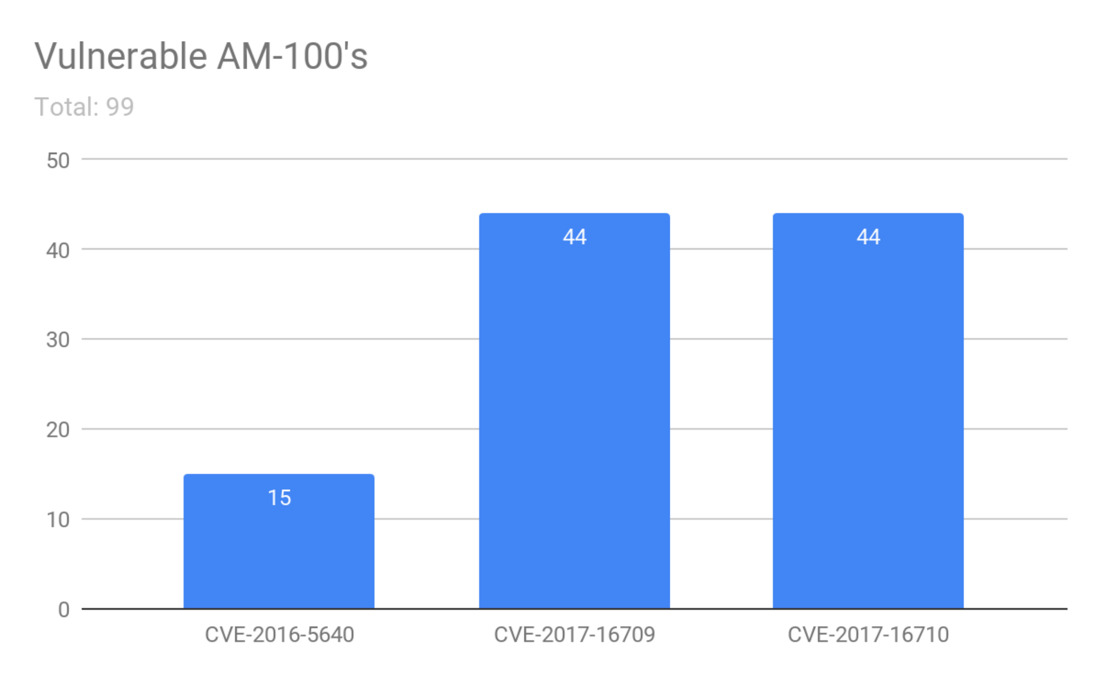
Copyright © 2018. All Rights Reserved

Crestron Air Media Data

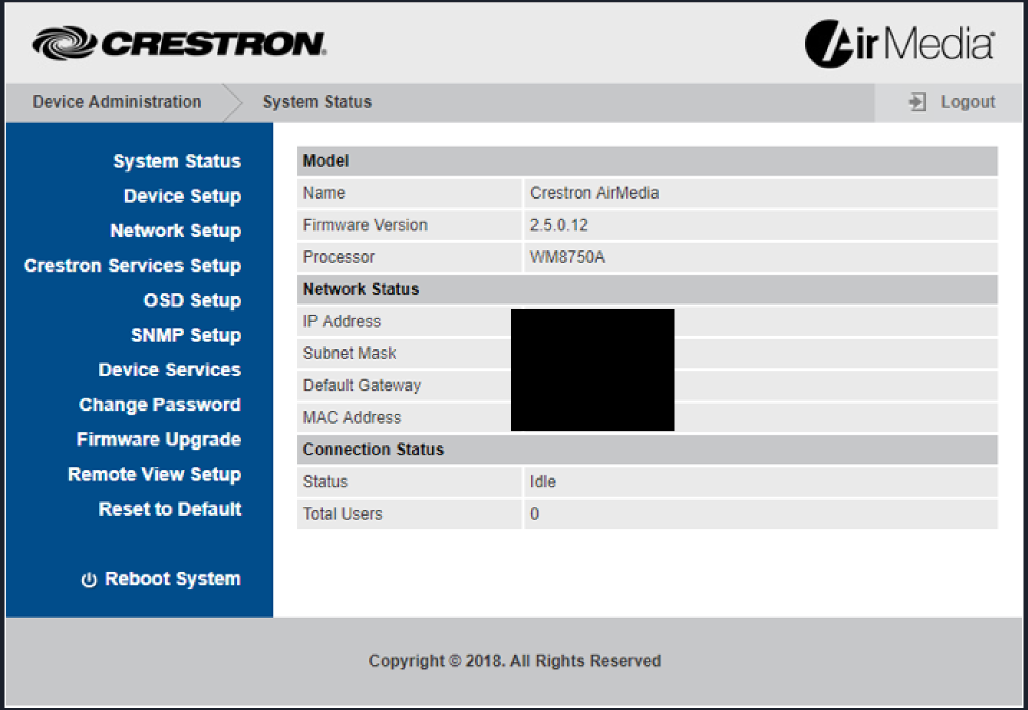


Past Vulnerabilities

- CVE-2016-5640 (AM-100/101)
  - Directory Traversal /RCE
  - Firmware < 1.2.1
- CVE-2017-16709 (AM-100/101)
  - RCE Vulnerability
  - Firmware < 1.6.0 / 2.7.0
- CVE-2017-16710 (AM-100/101)
  - XSS Vulnerability
  - Firmware < 1.6.0 / 2.7.0
- **83% Vulnerable**



Crestron Air Media

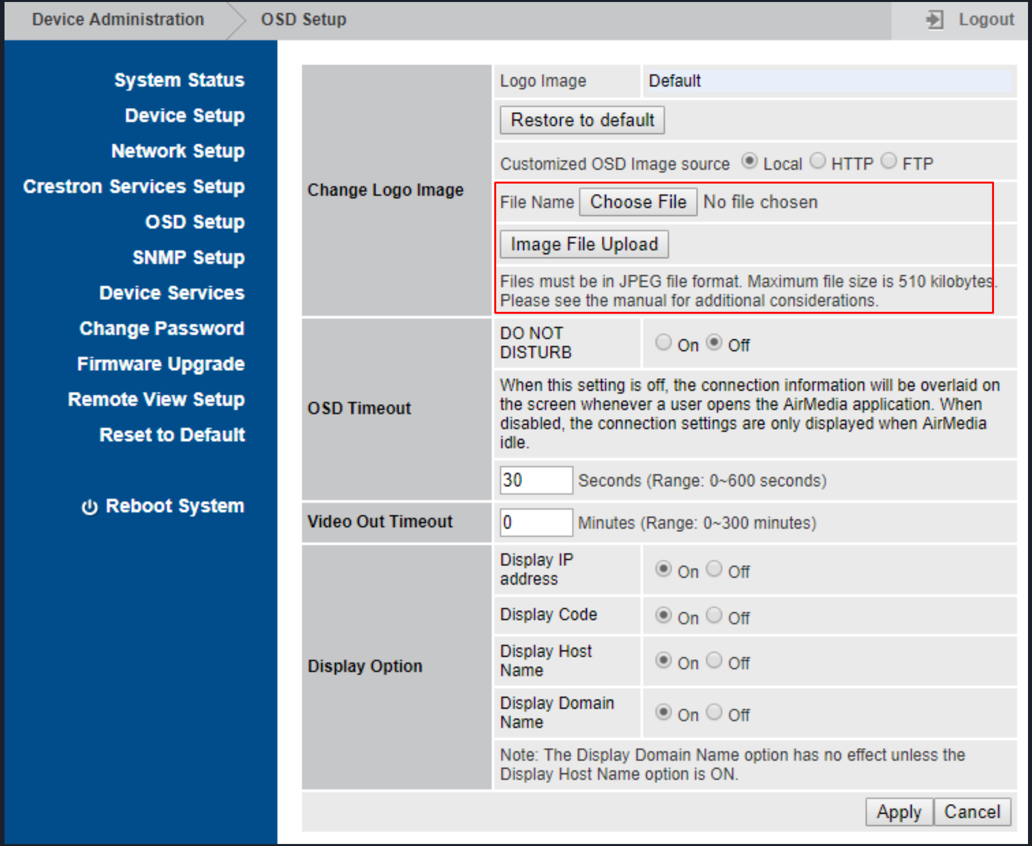


Model	
Name	Crestron AirMedia
Firmware Version	2.5.0.12
Processor	WM8750A
Network Status	
IP Address	[redacted]
Subnet Mask	
Default Gateway	
MAC Address	
Connection Status	
Status	Idle
Total Users	0

Copyright © 2018. All Rights Reserved

- Default Open Ports 80, 443, 161, 515, 5353
- Default passwords

Shenanigans!



Change Logo Image

Logo Image: Default

Restore to default

Customized OSD Image source ● Local ○ HTTP ○ FTP

File Name Choose File No file chosen

Image File Upload

Files must be in JPEG file format. Maximum file size is 510 kilobytes. Please see the manual for additional considerations.

OSD Timeout

DO NOT DISTURB ○ On ● Off

When this setting is off, the connection information will be overlaid on the screen whenever a user opens the AirMedia application. When disabled, the connection settings are only displayed when AirMedia idle.

30 Seconds (Range: 0~600 seconds)

Video Out Timeout: 0 Minutes (Range: 0~300 minutes)

Display Option

Display IP address ● On ○ Off

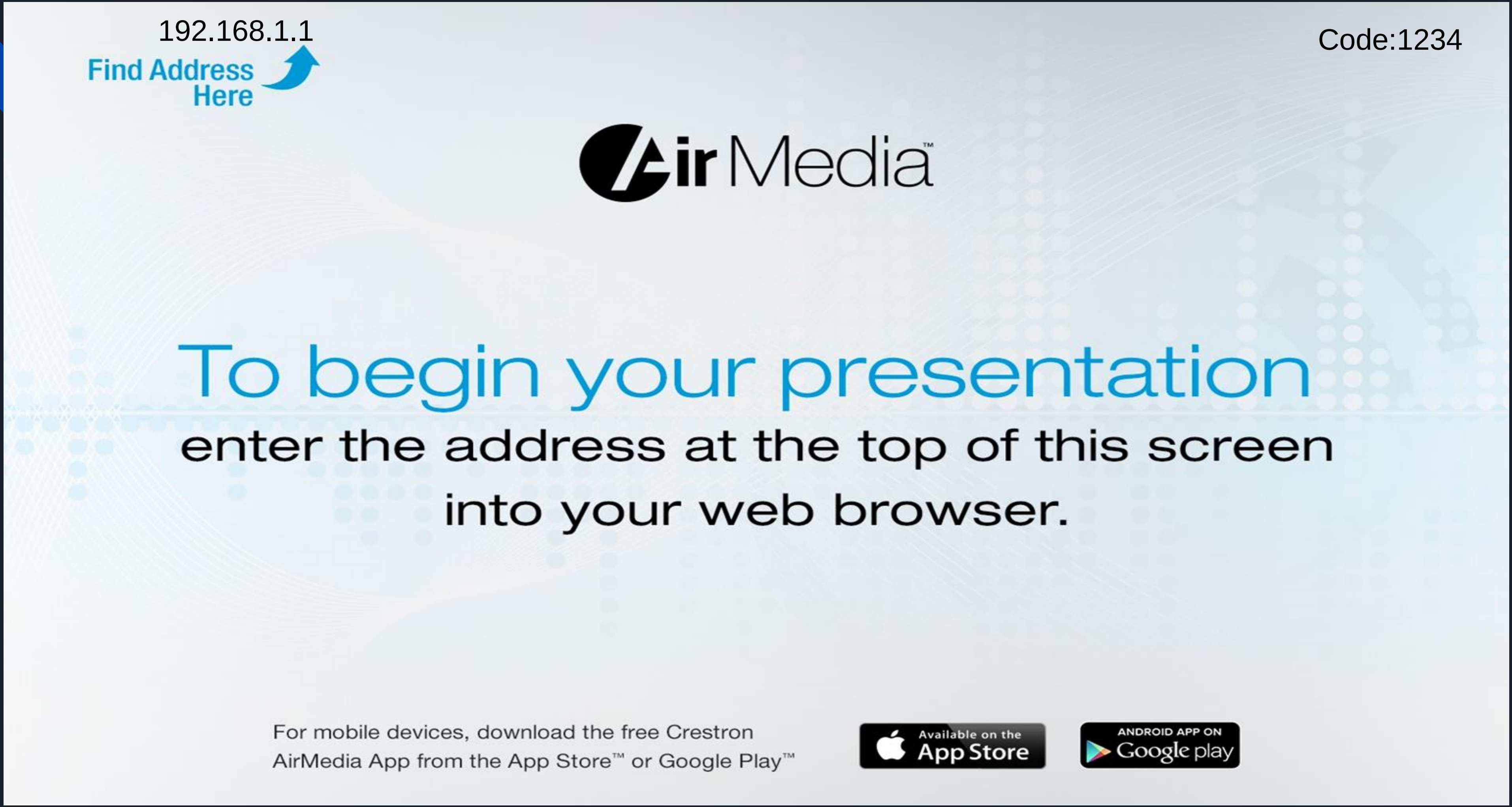
Display Code ● On ○ Off

Display Host Name ● On ○ Off

Display Domain Name ● On ○ Off

Note: The Display Domain Name option has no effect unless the Display Host Name option is ON.

Apply Cancel



192.168.1.1

Find Address Here

Code:1234

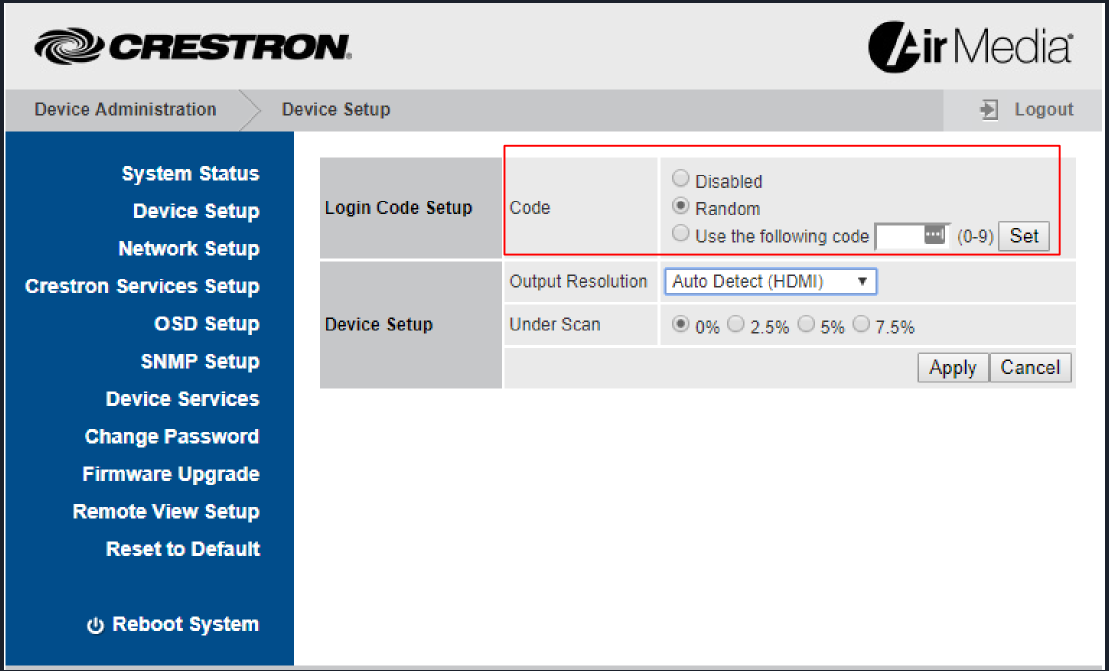
AirMedia™

To begin your presentation

enter the address at the top of this screen into your web browser.

For mobile devices, download the free Crestron AirMedia App from the App Store™ or Google Play™

Even further....



Login Code Setup	Code	○ Disabled ● Random ○ Use the following code (0-9)
Device Setup	Output Resolution	Auto Detect (HDMI)
	Under Scan	● 0% ○ 2.5% ○ 5% ○ 7.5%

1. Air Media authenticates users with 4 digit code
2. Disable code
3. Hack the planet

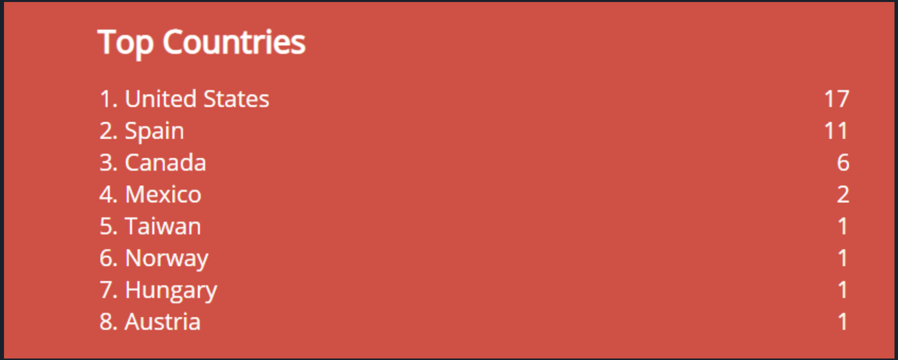
planking
is
DEADLY
[projector whirring]

Projectors

EPSON®
EXCEED YOUR VISION

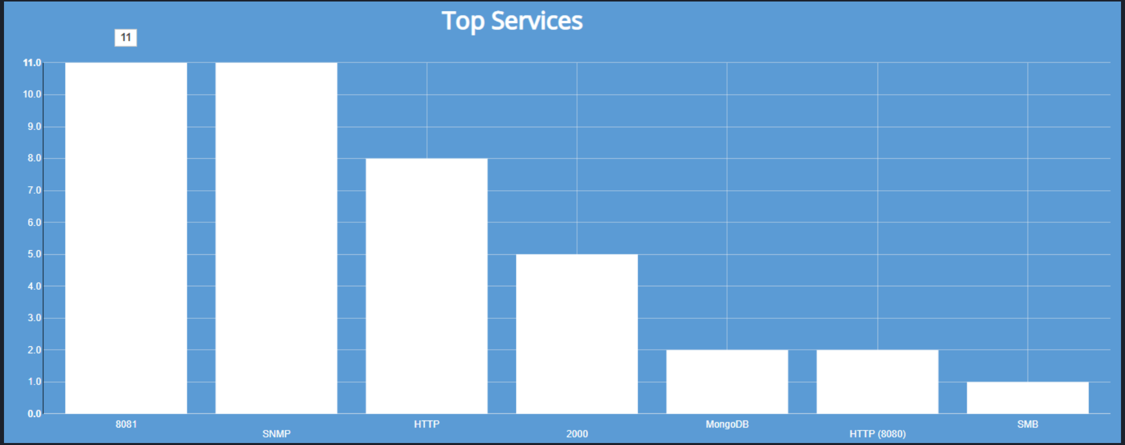
SONY

Network Projector DATA

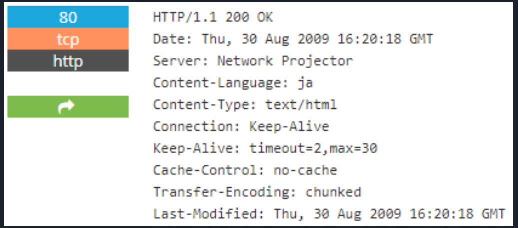


Top Countries

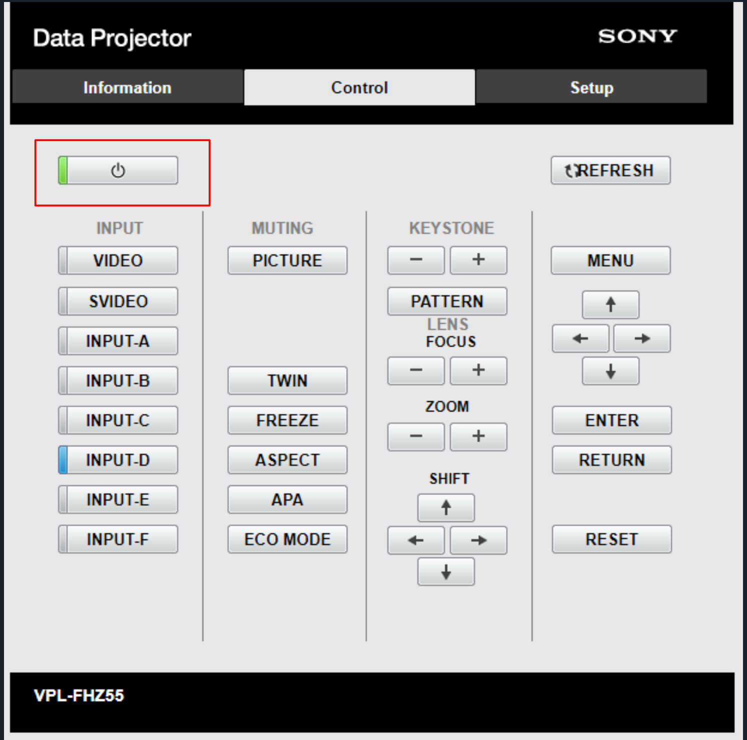
1. United States	17
2. Spain	11
3. Canada	6
4. Mexico	2
5. Taiwan	1
6. Norway	1
7. Hungary	1
8. Austria	1

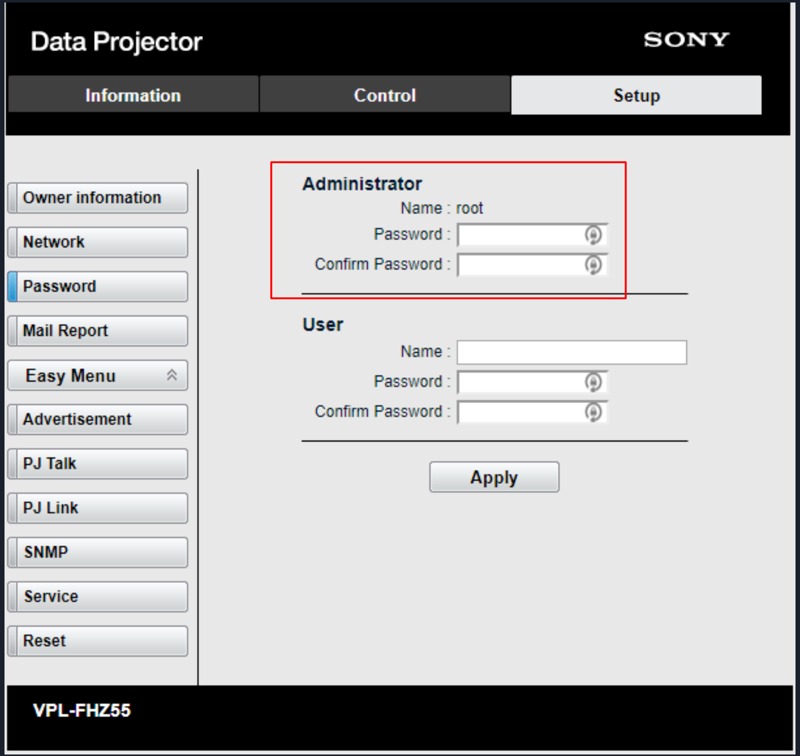


Sony Projectors



```
HTTP/1.1 200 OK
Date: Thu, 30 Aug 2009 16:20:18 GMT
Server: Network Projector
Content-Language: ja
Content-Type: text/html
Connection: Keep-Alive
Keep-Alive: timeout=2,max=30
Cache-Control: no-cache
Transfer-Encoding: chunked
Last-Modified: Thu, 30 Aug 2009 16:20:18 GMT
```





Administrator

Name : root

Password :

Confirm Password :

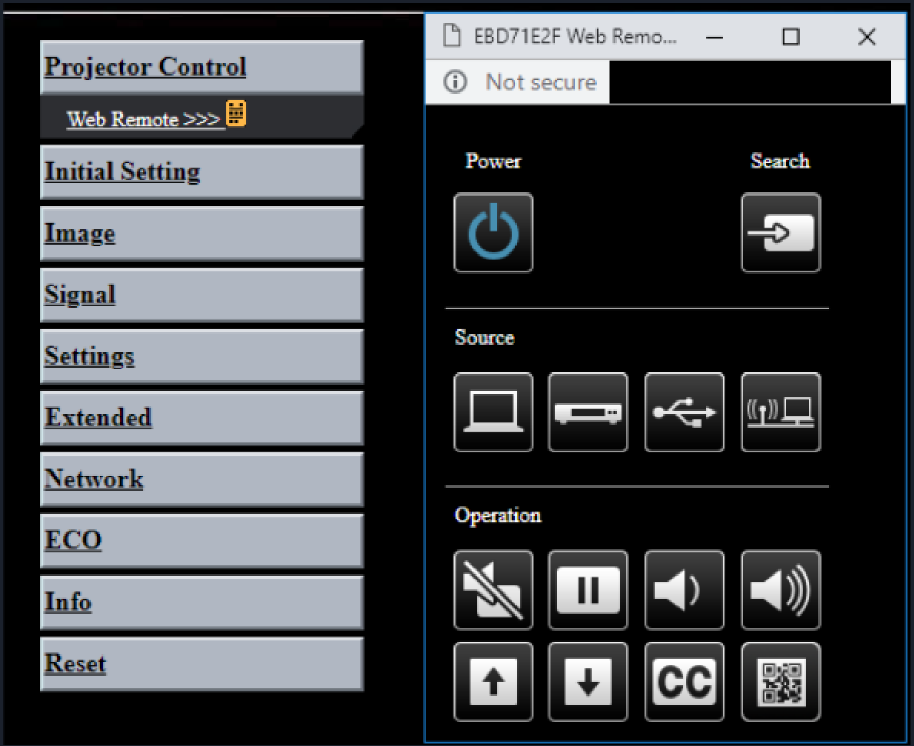
User

Name :

Password :

Confirm Password :

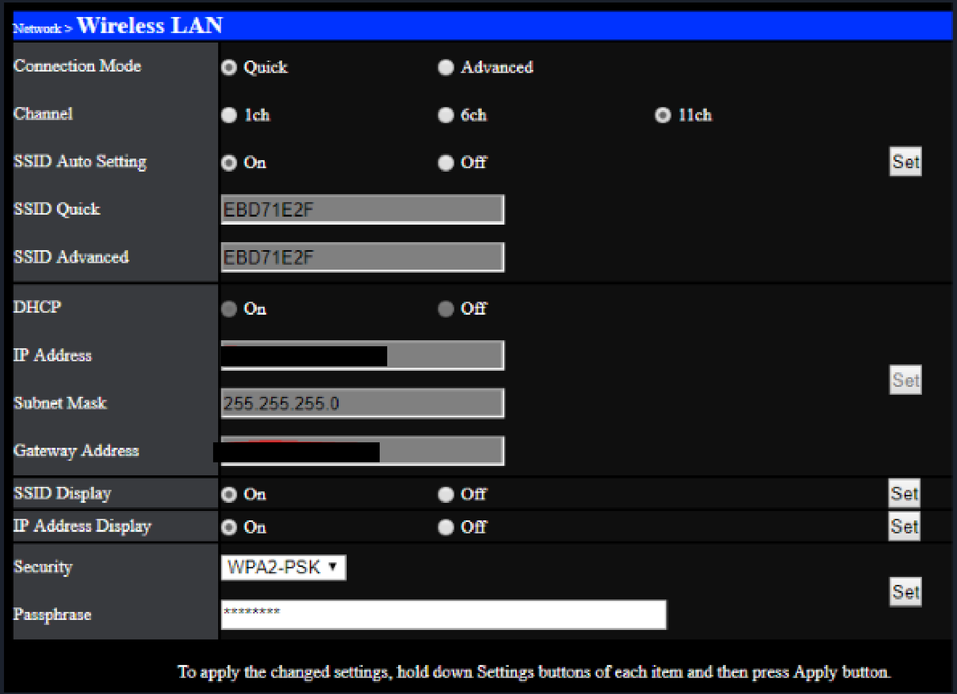
Epson Projector Web Control



- Power On/Off projector
- Change input
- Change projector settings
- Admin control

BOUNCINGDODECAHEDRONS.TUMBLR
Um, we have sort of a problem here.

Wi-fi Settings!



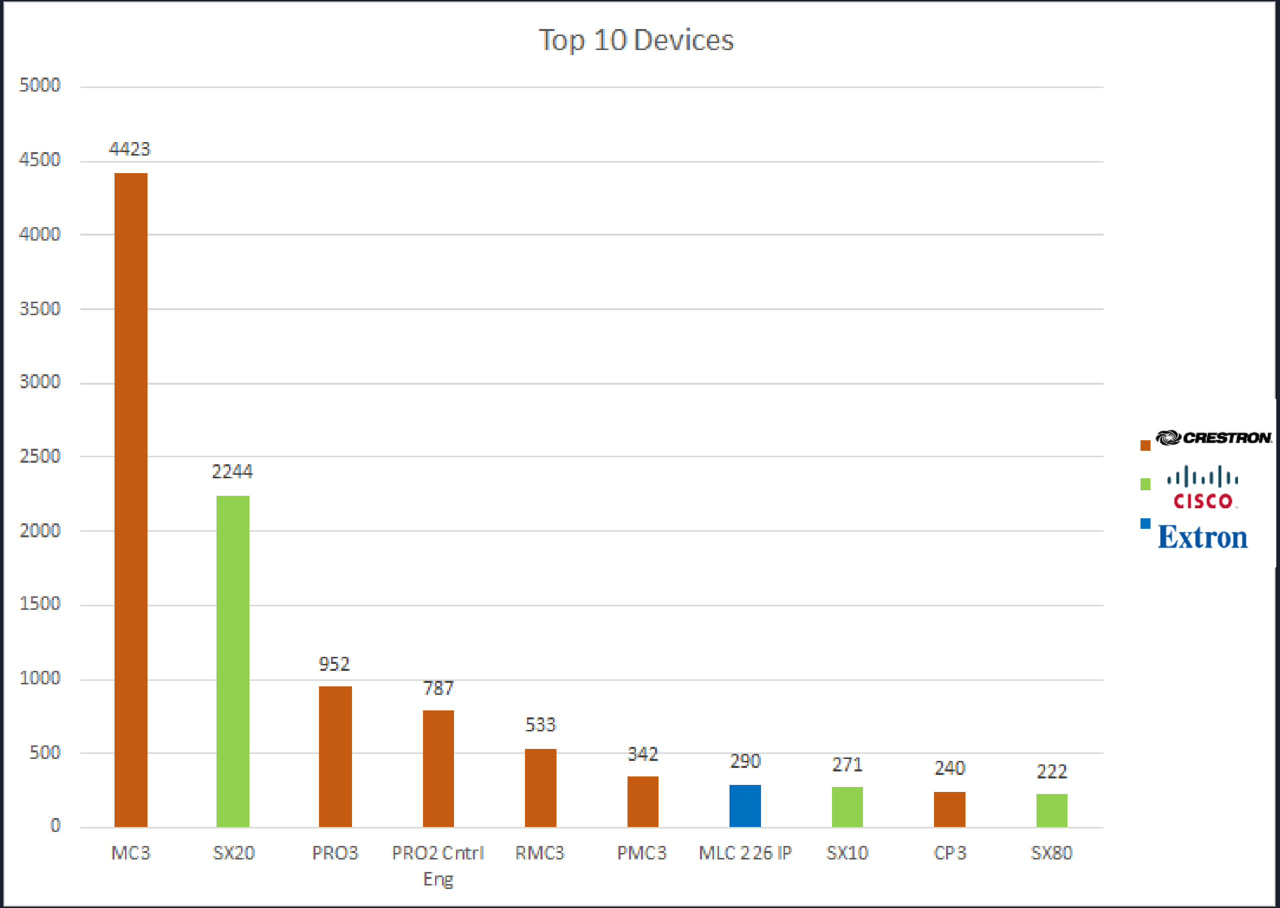
Network > **Wireless LAN**

Connection Mode	● Quick	○ Advanced		
Channel	○ 1ch	○ 6ch	● 11ch	
SSID Auto Setting	● On	○ Off		Set
SSID Quick	EBD71E2F			
SSID Advanced	EBD71E2F			
DHCP	○ On	○ Off		
IP Address	[redacted]			Set
Subnet Mask	255.255.255.0			
Gateway Address	[redacted]			
SSID Display	● On	○ Off		Set
IP Address Display	● On	○ Off		Set
Security	WPA2-PSK ▼			Set
Passphrase	*********			

To apply the changed settings, hold down Settings buttons of each item and then press Apply button.

Most Vulnerable Orgs

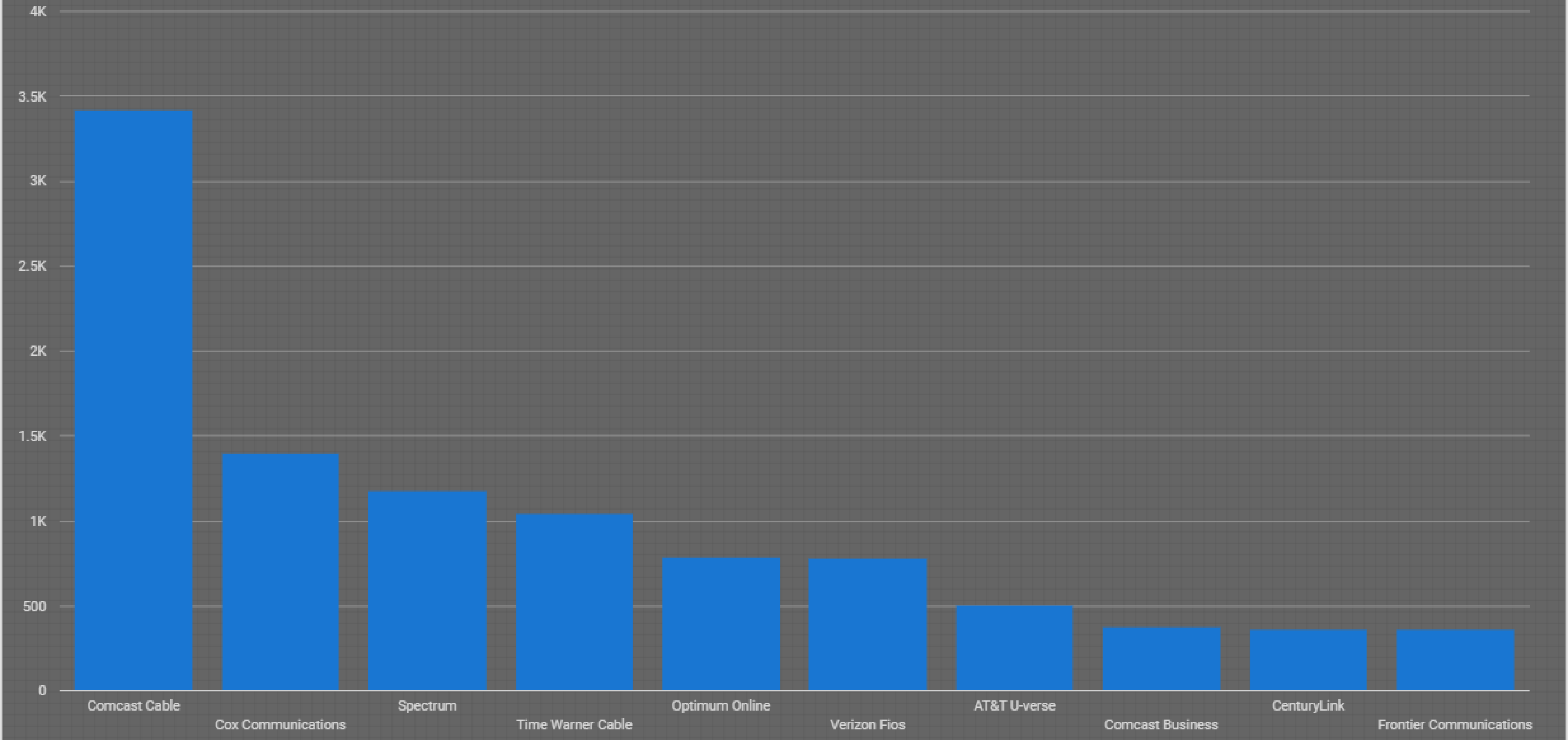
- Universities
- Small Businesses
- Understaffed/ Inexperienced AV/ IT Teams
- Legacy equipment



Top Organizations

Total Organizations
1,116

By: Anthony Tippy
Tibbbbz



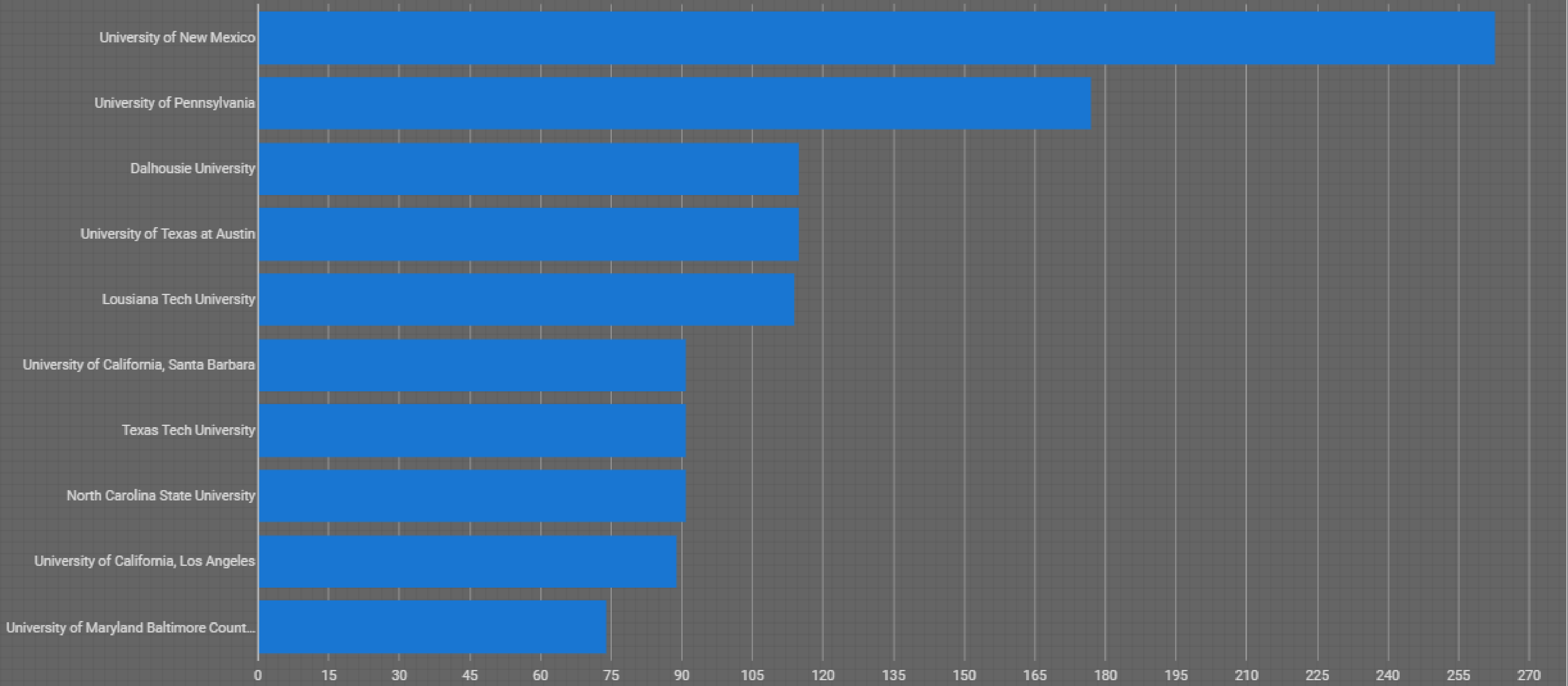
Top Universities

Total Count

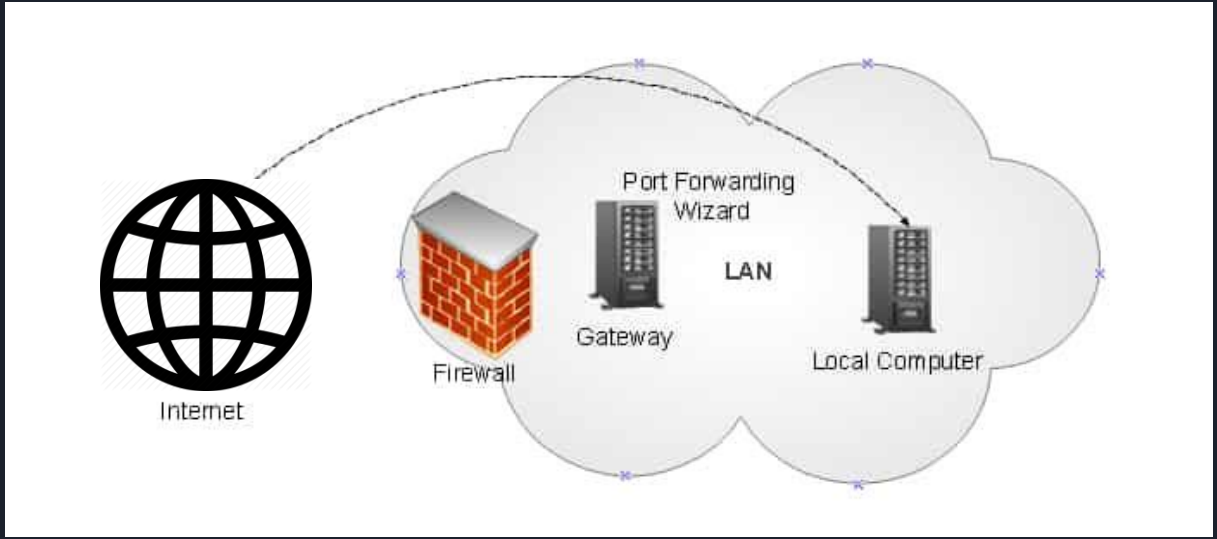
40

By: Anthony Tippy

Tibbbbz



UPnP – Automatic Port Forwarding



- Universal Plug n Play (UPnP) settings will often automatically forward ports on your network to the open internet

<u>How To Mitigate</u>

1. Select “Disable UPnP” in router settings/ devices
2. Disable Port Forwarding on your router
3. Routinely audit UPnP connections

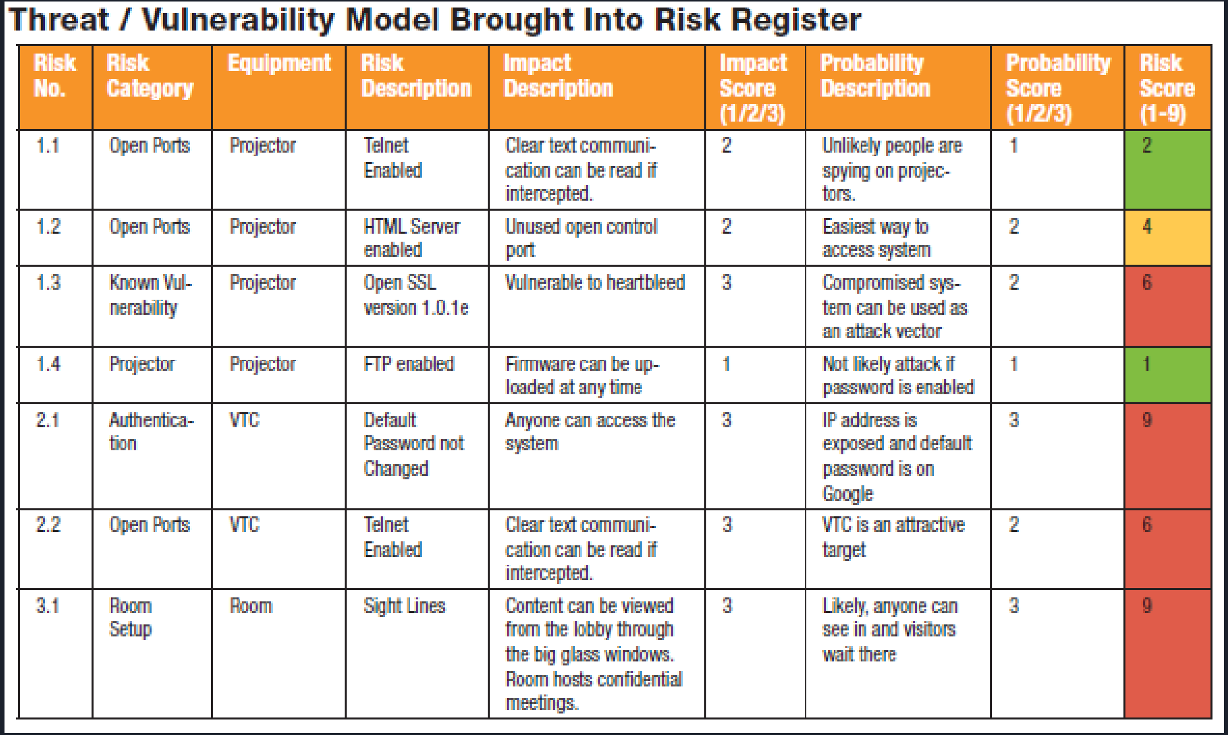
How do we secure our orgs? -Users

Basic Security Hygiene

1. STOP PUTTING DEVICES ONLINE
   a. Don’t connect it at all!
   b. Does it *REALLY* need to be on your network/the net
2. Authentication
   a. Default password/ easy password?
3. Security as a standard
   a. Security integrated into the development process
   b. Consistent and continual firmware upgrades/checks
4. Disable UPnP
5. Subnet your stuff
   a. Data over there, A/V tech over here
6. Physically secure technology in locked rack
7. Enable Audit logs

AV/IT Security by Design

- Vet products as part of design process
- Consider AV equipment within your threat model and risk assessment
- *If it connects to the network, its probably a risk you should consider*



Threat / Vulnerability Model Brought Into Risk Register

Risk No.	Risk Category	Equipment	Risk Description	Impact Description	Impact Score (1/2/3)	Probability Description	Probability Score (1/2/3)	Risk Score (1-9)
1.1	Open Ports	Projector	Telnet Enabled	Clear text communication can be read if intercepted.	2	Unlikely people are spying on projectors.	1	2
1.2	Open Ports	Projector	HTML Server enabled	Unused open control port	2	Easiest way to access system	2	4
1.3	Known Vulnerability	Projector	Open SSL version 1.0.1e	Vulnerable to heartbleed	3	Compromised system can be used as an attack vector	2	6
1.4	Projector	Projector	FTP enabled	Firmware can be uploaded at any time	1	Not likely attack if password is enabled	1	1
2.1	Authentication	VTC	Default Password not Changed	Anyone can access the system	3	IP address is exposed and default password is on Google	3	9
2.2	Open Ports	VTC	Telnet Enabled	Clear text communication can be read if intercepted.	3	VTC is an attractive target	2	6
3.1	Room Setup	Room	Sight Lines	Content can be viewed from the lobby through the big glass windows. Room hosts confidential meetings.	3	Likely, anyone can see in and visitors wait there	3	9

Phones/ Communication

- Diligent monitoring through RMS
  - Firmware upgrades
- Minimize open ports/ services
- VLAN to separate voice traffic from data
- End to end encryption
- PATCH PATCH PATCH PATCH!

Video Conferencing

- Enable encryption on calls
- Disable broadcast streaming
- Disable far end camera control
- Disable auto-answer feature
- Monitor technology with management software
  - AMX RMS, Cisco UCMS
  - Has audit logs for events/incidents

What can you do?- Manufacturers

Security by default/Design

- No more *default* passwords for devices
  - California is enacting this to law by 2020
- Disable unnecessary ports by default
- Web interfaces need passwords
- Automatic firmware updates (need network)
- Triggered alerts
  - Upon outage, or error
- Audit logs
- Properly Designed UPnP usage

Top Strategies to Secure Your Organization

1. Your firewall should NOT be open (Check UPnP)
2. Device management software for ALL networked A/V devices
3. Robust passwords for maintenance/ Service
4. Include A/V devices within your IPS/IDS system
5. Vet A/V products for security issues/ vulnerabilities before design / installation
6. Encryption on communications
7. Lock/ restrict access to physical equipment

Thank You’s

- MiSec Community
- Shodan
- GrrCon Community
- Inspiration from Dan Tentler’s talks on Shodan
    - *“115 batshit stupid things you can put on the internet in as fast as I can go”*
    - *“Drinking from the caffeine firehose we know as shodan”*
- Ricky ‘HeadlessZeke’ Lawshae - *“Who Controls the Controllers Hacking Crestron”*

BONUS: Crestron Smart Home!?- PYNG-HUB

Can Control:

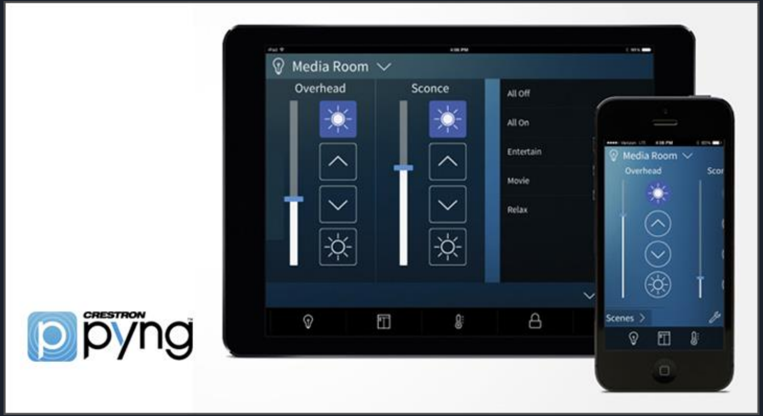
-Lights

-doors

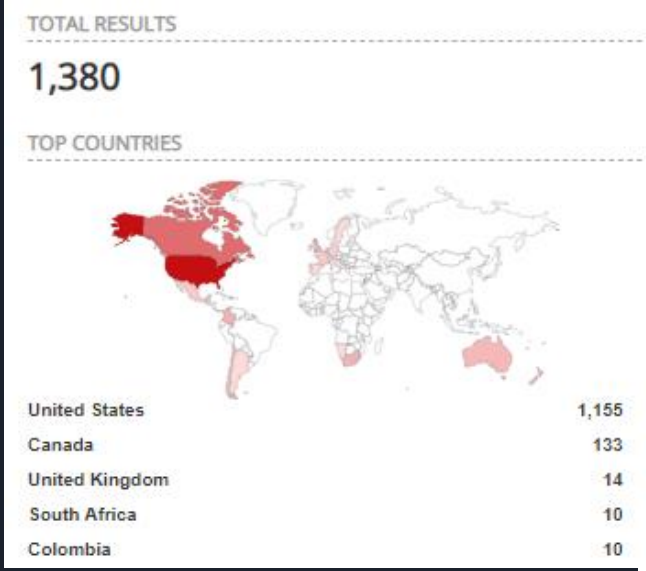
-thermostat

-TV’s/ Media sources

-Touch Panels



PYNG-HUB Query

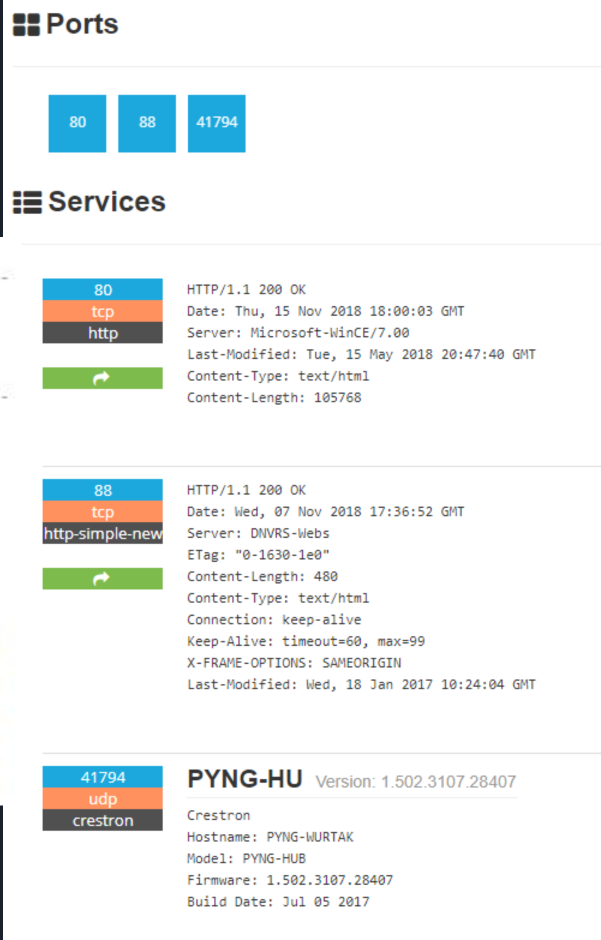


TOTAL RESULTS

1,380

TOP COUNTRIES

United States	1,155
Canada	133
United Kingdom	14
South Africa	10
Colombia	10



Ports

80 88 41794

Services

80 tcp http

```
HTTP/1.1 200 OK
Date: Thu, 15 Nov 2018 18:00:03 GMT
Server: Microsoft-WinCE/7.00
Last-Modified: Tue, 15 May 2018 20:47:40 GMT
Content-Type: text/html
Content-Length: 105768
```

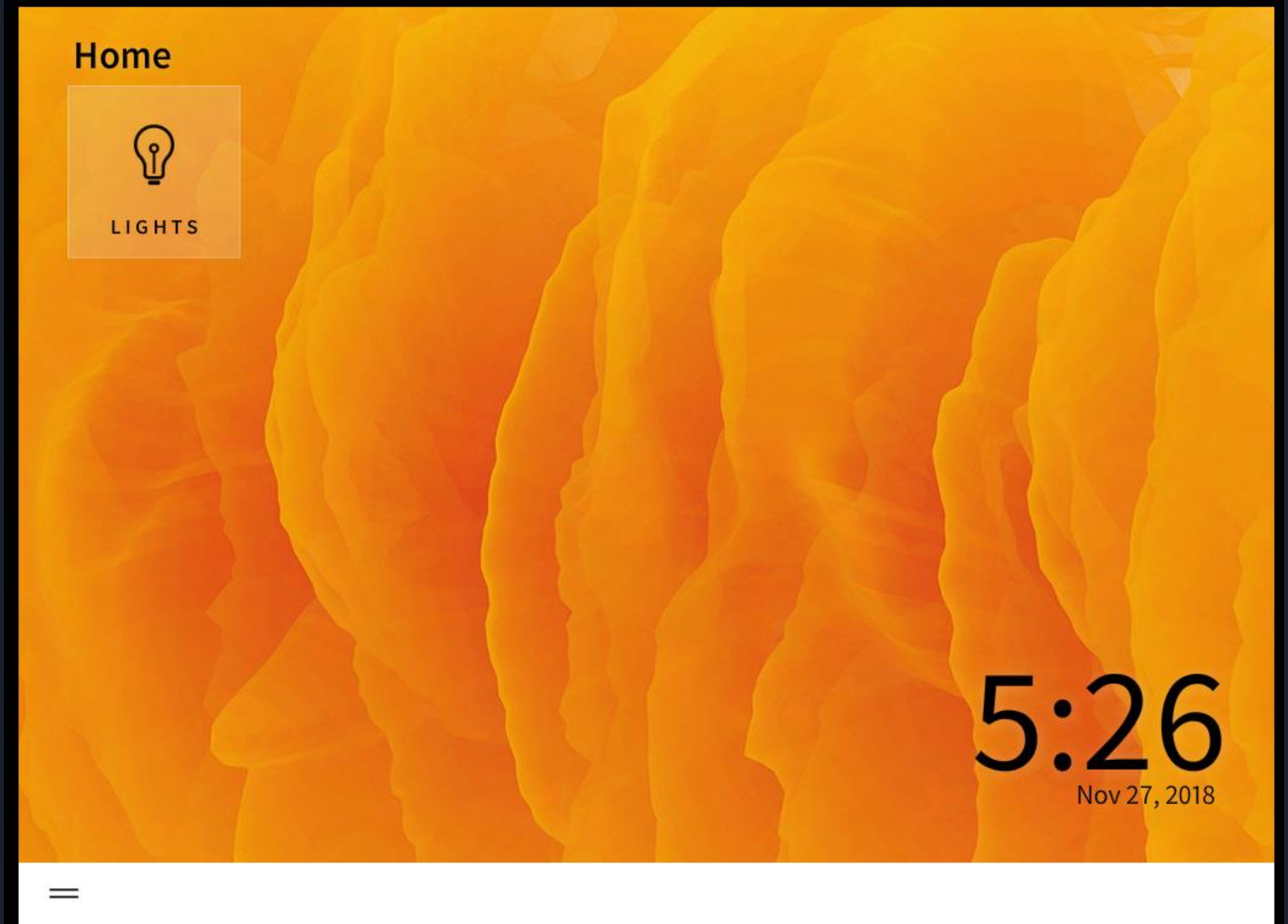
88 tcp http-simple-new

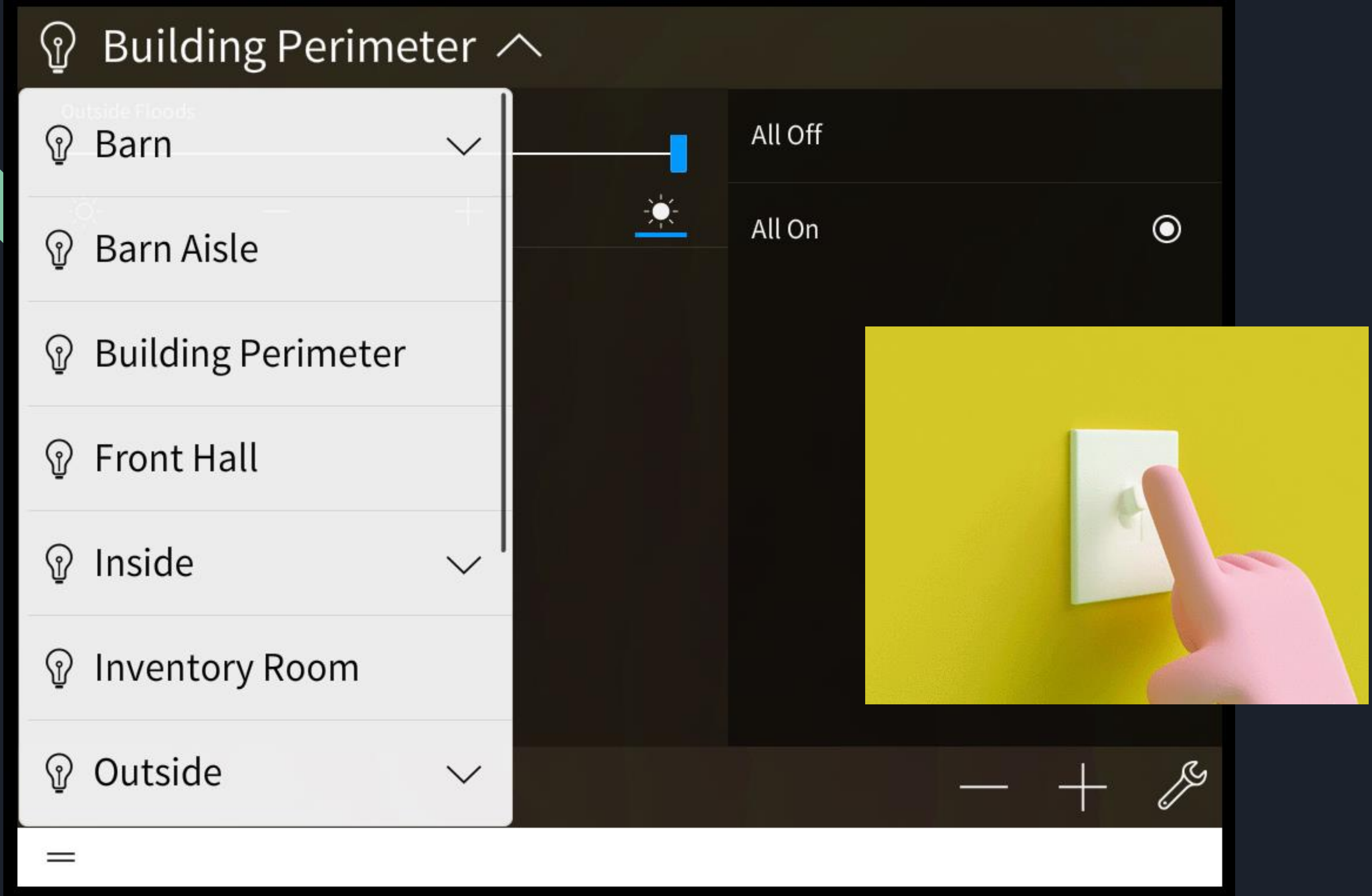
```
HTTP/1.1 200 OK
Date: Wed, 07 Nov 2018 17:36:52 GMT
Server: DNVRS-Webs
ETag: "0-1630-1e0"
Content-Length: 480
Content-Type: text/html
Connection: keep-alive
Keep-Alive: timeout=60, max=99
X-FRAME-OPTIONS: SAMEORIGIN
Last-Modified: Wed, 18 Jan 2017 10:24:04 GMT
```

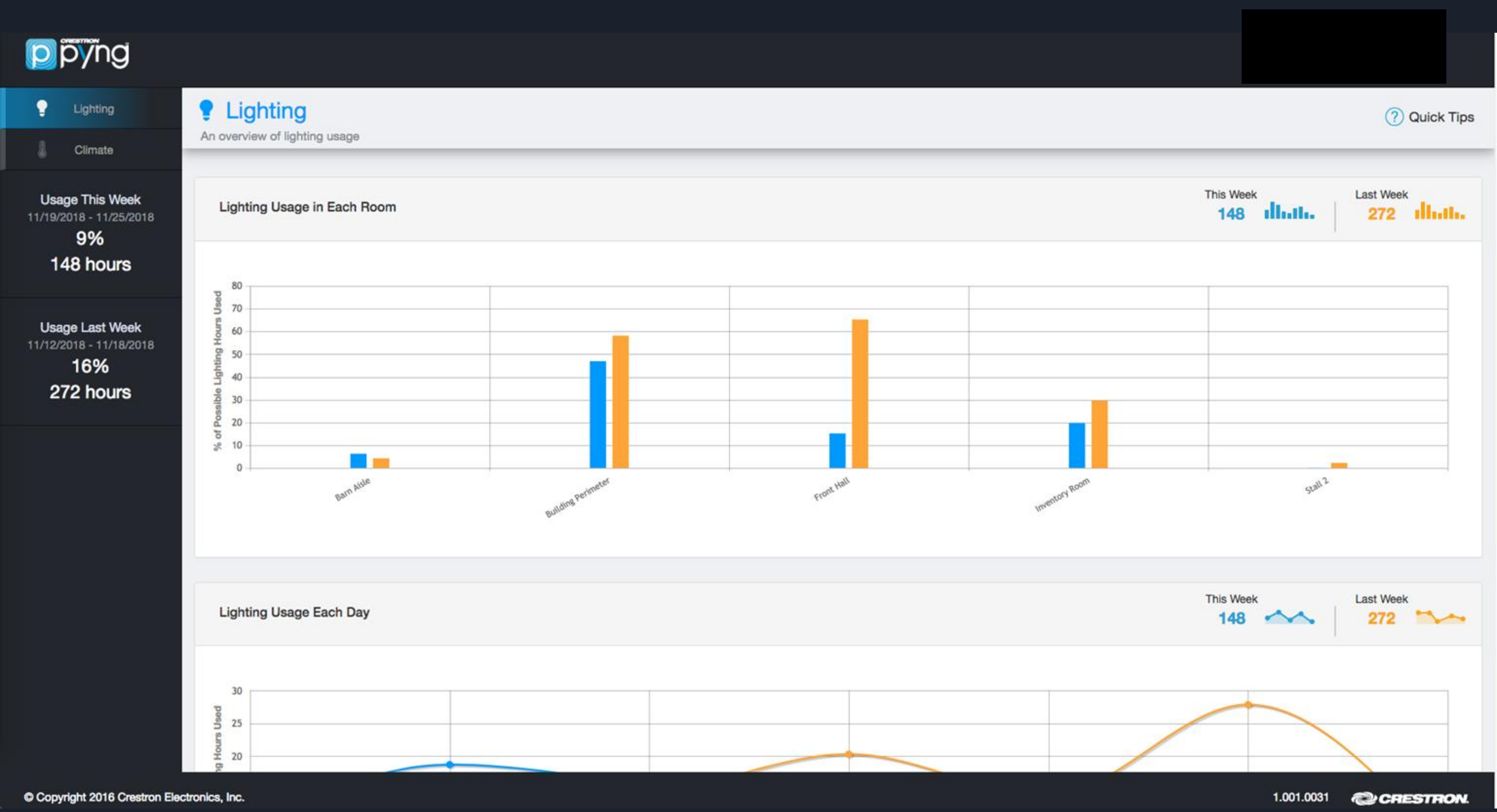
41794 udp crestron

PYNG-HU Version: 1.502.3107.28407

```
Crestron
Hostname: PYNG-WURTAK
Model: PYNG-HUB
Firmware: 1.502.3107.28407
Build Date: Jul 05 2017
```


Home
LIGHTS
5:26
Nov 27, 2018


Building Perimeter
Outside Floods
Barn
Barn Aisle
Building Perimeter
Front Hall
Inside
Inventory Room
Outside
All Off
All On ◉



[redacted]

Lighting

Climate

Usage This Week
11/19/2018 - 11/25/2018
9%
148 hours

Usage Last Week
11/12/2018 - 11/18/2018
16%
272 hours

Lighting
An overview of lighting usage

Quick Tips

Lighting Usage in Each Room

This Week 148

Last Week 272

Lighting Usage Each Day

This Week 148

Last Week 272

© Copyright 2016 Crestron Electronics, Inc.

1.001.0031

FIN