FROM HARDWARE TO 0-DAY

OR HOW TO BUY A SECURITY CAMERA AND NEVER USE IT FOR ITS INTENDED PURPOSE

PIETRO OLIVA

WHOAMI

- NAME: PIETRO OLIVA
- TWITTER: @0XSYSENTER
- CURRENT ROLE: SECURITY RESEARCHER (R3)
- PREVIOUS ROLES:
  - SECURITY RESEARCHER (SONY)
  - RED TEAM OPERATOR (JP MORGAN)
  - PENETRATION TESTER / SECURITY AUDITOR (NCC GROUP, PWC, GMV)

AGENDA

- WHY PERFORM SECURITY RESEARCH ON A SECURITY CAMERA
- INFORMATION GATHERING ON PREVIOUS WORK
- THE CHALLENGE
- THE PATH TO SUCCESS
- LESSONS LEARNED
- FUTURE WORK
- CONCLUSIONS
- Q & A

WHY PERFORM SECURITY RESEARCH ON A SECURITY CAMERA?

- MANY PEOPLE SAY "IOT DEVICES ARE NOT SECURE"
- I WANTED TO VERIFY THESE CLAIMS
- I WAS LOOKING FOR A CHALLENGE AND LEARNING OPPORTUNITY

Pietro Oliva – @0xsysenter

PREVIOUS WORK ON TP-LINK NC200/NC220

- THIS WAS ALREADY PATCHED ON LATER FIRMWARE VERSIONS
- IS THERE REALLY ONLY ONE VULNERABILITY AFFECTING THIS CAMERA?

IOActive Security Advisory

Title	Authenticated OS Command Injection on TP-LINK Cloud Cameras
Severity	High – CVSSv2 Score 6.0 (AV:L/AC:H/Au:S/C:C/I:C/A:C)
Discovered by	Tao Sauvage
Advisory Date	March 9, 2016

Affected Products

1. TP-LINK Cloud Camera NC200, firmware NC200_V1_151125
2. TP-LINK Cloud Camera NC220, firmware NC220_V1_151125

Impact

An attacker with Administrator (admin) access to the administrative web panel of a TP-LINK Cloud Camera can gain root access to the device, fully compromising its confidentiality, integrity, and availability.

Background

TP-LINK Cloud Cameras offer a quick and easy way to “See there, when you can’t be there,” allowing users to remotely monitor everything going on where the cameras are installed. TP-LINK Cloud Cameras allow video monitoring and recording, which can later be accessed from around the world thanks to the TP-LINK Cloud service.

Technical Details

The administrative web panel allows the admin to configure PPPoE on the Cloud Camera device. IOActive found that the username and password fields were vulnerable to OS command injection, which would allow an attacker to execute OS commands on the device with root privileges.

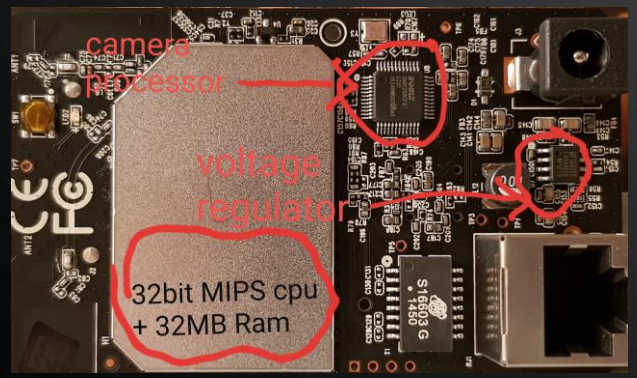
THE CHALLENGE

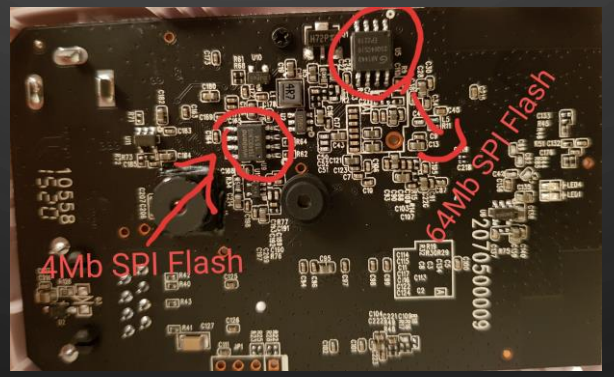
HACK THE LATEST AND GREATEST FIRMWARE

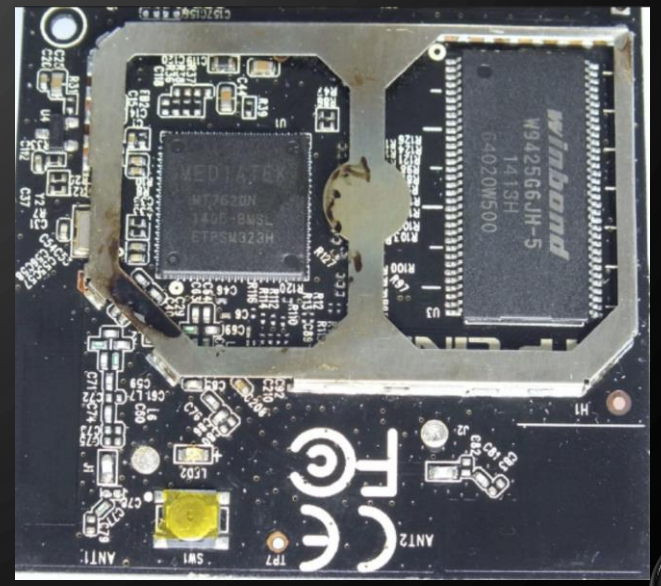
- STARTING FROM HARDWARE ANALYSIS AND FIRMWARE DUMPING
- BY PERFORMING FIRMWARE REVERSE ENGINEERING (DELIBERATELY EXCLUDING FUZZING)
- ON AN ARCHITECTURE I WAS UNFAMILIAR WITH (MIPS)
- USING A REVERSE ENGINEERING TOOL THAT:
  - IS FREE AND OPEN SOURCE
  - I CAN USE EVERYWHERE (INCLUDING ON A MOBILE PHONE)
- THAT TOOL EXISTS AND IS CALLED RADARE2!

HARDWARE ANALYSIS AND FLASH DUMPING

- IDENTIFIED THE BOARD COMPONENTS VIA PICTURES AND FCC ID
- DOWNLOADED DATASHEETS
- PERFORMED FLASH DUMPING



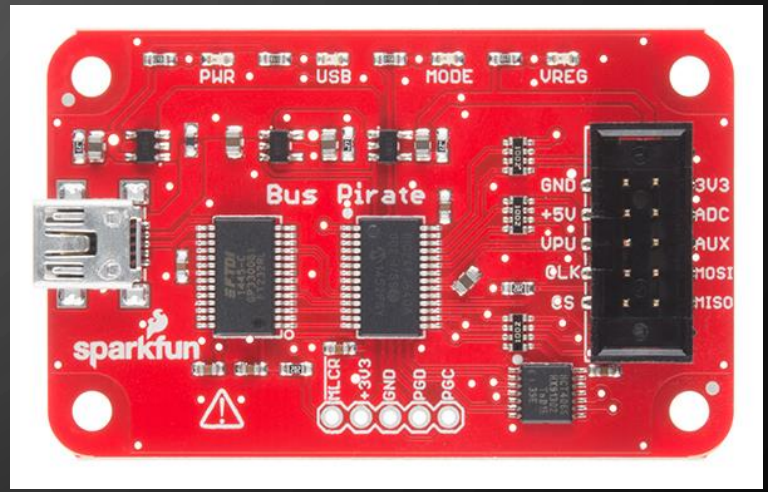




RZCON 2020

SPI FLASH DUMPING – TOOLS

- BUS PIRATE AS SPI READER/WRITER
- FLASHROM TO PERFORM DUMP VIA BUS PIRATE
- THE 8 MB SPI FLASH CONTAINED THE MAIN FIRMWARE!



FIRMWARE EXTRACTION AND ANALYSIS

- BINWALK + JEFFERSON FOR FILESYSTEM EXTRACTION
- RADARE2 AS THE MAIN REVERSE ENGINEERING TOOL
- MAIN REVERSE ENGINEERING TARGET: A BINARY CALLED “IPCAMERA”

RZCON 2020

BUGS, BUGS, BUGS…

CVE-2020-10231 - TP-LINK CLOUD CAMERAS NCXXX REMOTE NULL POINTER DEREFERENCE

```
0x0047dca0      2800c48f        lw a0, (arg_user)
0x0047dca4      2c00c58f        lw a1, (arg_password)
0x0047dca8      208e998f        lw t9, -sym.swUMMatchPassword(gp) ; [0x534130:4]=0x4bdf68 sym.swUMMatchPassword ; "h\xdfK"
0x0047dcac      00000000        nop
0x0047dcb0      09f82003        jalr t9
0x0047dcb4      00000000        nop
0x0047dcb8      2000dc8f        lw gp, (arg_20h)
0x0047dcbc      5000c2af        sw v0, (arg_50h)
0x0047dcc0      5000c28f        lw v0, (arg_50h)
0x0047dcc4      00000000        nop
0x0047dcc8      5a004014        bnez v0, 0x47de34
0x0047dccc      00000000        nop
0x0047dcd0      5400c0af        sw zero, (arg_54h)
0x0047dcd4      7800c48f        lw a0, (http_env)
0x0047dcd8      1c80858f        lw a1, -0x7fe4(gp)          ; [0x53332c:4]=0x4f0000 "uldn't find protocol block."
0x0047dcdc      00000000        nop
0x0047dce0      5083a524        addiu a1, a1, -0x7cb0       ; 0x4e8350 ; "HTTP_USER_AGENT" ; str.HTTP_USER_AGENT
0x0047dce4      0483998f        lw t9, -sym.httpGetEnv(gp)  ; [0x533614:4]=0x45d0f8 sym.httpGetEnv
0x0047dce8      00000000        nop
0x0047dcec      09f82003        jalr t9
0x0047dcf0      00000000        nop
0x0047dcf4      2000dc8f        lw gp, (arg_20h)
0x0047dcf8      5800c2af        sw v0, (arg_58h)
0x0047dcfc      5800c48f        lw a0, (arg_58h)
0x0047dd00      1c80858f        lw a1, -0x7fe4(gp)          ; [0x53332c:4]=0x4f0000 "uldn't find protocol block."
0x0047dd04      00000000        nop
0x0047dd08      6083a524        addiu a1, a1, -0x7ca0       ; 0x4e8360 ; "Firefox" ; str.Firefox
0x0047dd0c      c089998f        lw t9, -sym.imp.strstr(gp)  ; [0x533cd0:4]=0x4dd380 sym.imp.strstr
0x0047dd10      00000000        nop
0x0047dd14      09f82003        jalr t9
```

RZCON 2020

THE PAIN OF RESPONSIBLE DISCLOSURE

CVE-2020-10231 - TP-LINK CLOUD CAMERAS NCXXX REMOTE NULL POINTER DEREFERENCE

- STAGE 1 (4TH DECEMBER 2019): THE CAMERA IS "NOT SUPPORTED ANYMORE"
- STAGE 2 (FEBRUARY 2020): LET'S SEE IF OTHER CAMERAS ARE AFFECTED
- STAGE 3 (24TH FEBRUARY 2020): WARN THE VENDOR ALL NC CAMERAS ARE AFFECTED
- STAGE 4 (29TH MARCH 2020): DROP A ZERO DAY
- STAGE 6 (8TH APRIL 2020): VULNERABILITY GETS FIXED
- STAGE 5 (MULTIPLE DATES): NEXT REPORTS AND DEADLINES ARE TAKEN SERIOUSLY
- STAGE 7 (7TH MAY 2020): PROMISED I WON'T REPORT ANY MORE ISSUES

BUGS, BUGS, BUGS…

CVE-2020-13224 - TP-LINK CLOUD CAMERAS NCXXX DELMULTIUSER STACK OVERFLOW

```
0x0047ebd0    4404c48f    lw a0, (arg_usernames_copy)
0x0047ebd4    0086998f    lw t9, -sym.swUMDelUser(gp) ; [0x533910:4]=0x4c0708 sym.swUMDelUser
0x0047ebd8    00000000    nop
0x0047ebdc    09f82003    jalr t9
0x0047ebe0    00000000    nop
0x0047ebe4    1000dc8f    lw gp, (arg_10h)
0x0047ebe8    1800c2af    sw v0, (error_code)
0x0047ebec    4804c227    addiu v0, fp, 0x448
0x0047ebf0    21204000    move a0, v0
0x0047ebf4    1c80858f    lw a1, -0x7fe4(gp)          ; [0x53332c:4]=0x4f0000
0x0047ebf8    00000000    nop
0x0047ebfc    6c84a524    addiu a1, a1, -0x7b94       ; esilref: '{"errorCode":%d},'
0x0047ec00    1800c68f    lw a2, (error_code)
0x0047ec04    b485998f    lw t9, -sym.imp.sprintf(gp) ; [0x5338c4:4]=0x4dd740 sym.imp.sprintf
0x0047ec08    00000000    nop
0x0047ec0c    09f82003    jalr t9
0x0047ec10    00000000    nop
0x0047ec14    1000dc8f    lw gp, (arg_10h)
0x0047ec18    4000c227    addiu v0, fp, 0x40
0x0047ec1c    4804c327    addiu v1, fp, 0x448
0x0047ec20    21204000    move a0, v0
0x0047ec24    21286000    move a1, v1
0x0047ec28    308b998f    lw t9, -sym.imp.strcat(gp)  ; [0x533e40:4]=0x4dd270 sym.imp.strcat ; "p\xd2M"
0x0047ec2c    00000000    nop
0x0047ec30    09f82003    jalr t9
0x0047ec34    00000000    nop
0x0047ec38    1000dc8f    lw gp, (arg_10h)
0x0047ec3c    4004c28f    lw v0, (next_comma)
0x0047ec40    00000000    nop
0x0047ec44    01004224    addiu v0, v0, 1
0x0047ec48    1e000010    b 0x47ecc4
```

```
; CODE XREF from sym.httpDelMultiUserRpm @ 0x47ec48
0x0047ecc4    4004c28f    lw v0, (next_comma)
0x0047ecc8    00000000    nop
0x0047eccc    03004010    beqz v0, 0x47ecdc
0x0047ecd0    00000000    nop
0x0047ecd4    afff0010    b 0x47eb94
```

The PoC:

Usernames=,,

Pietro Oliva – @0xsysenter

BUGS, BUGS, BUGS…

CVE-2020-12110 - TP-LINK CLOUD CAMERAS NCXXX HARDCODED ENCRYPTION KEY (1)

```
0x004a1c54      1c80848f      lw a0, -0x7fe4(gp)
0x004a1c58      00000000      nop
0x004a1c5c      44b48424      addiu a0, a0, -0x4bbc       ; 0x4eb444 ; "/usr/local/config/ipcamera/pBackup"
0x004a1c60      1c80858f      lw a1, -0x7fe4(gp)
0x004a1c64      00000000      nop
0x004a1c68      d4b3a524      addiu a1, a1, -0x4c2c       ; 0x4eb3d4 ; "tp-link" ; str.tp_link
0x004a1c6c      1c80868f      lw a2, -0x7fe4(gp)
0x004a1c70      00000000      nop
0x004a1c74      7cb4c624      addiu a2, a2, -0x4b84       ; 0x4eb47c ; "/usr/local/config/ipcamera/eBackup"
0x004a1c78      0c88998f      lw t9, -sym.DES_Encrypt(gp) ; [0x533b1c:4]=0x497254 sym.DES_Encrypt
0x004a1c7c      00000000      nop
0x004a1c80      09f82003      jalr t9
```

BUGS, BUGS, BUGS…

CVE-2020-12110 - TP-LINK CLOUD CAMERAS NCXXX HARDCODED ENCRYPTION KEY (2)

THIS LOOKS STRAIGHTFORWARD, BUT WE HAVE A PROBLEM TO SOLVE:

- WE KNOW THE ALGORITHM IS DES ECB AND THE ENCRYPTION KEY
- FOUND A TOOL THAT WOULD CORRECTLY ENCRYPT/DECRYPT BACKUP FILES
- BUT I WOULD GET RANDOM DATA WITH STANDARD DES IMPLEMENTATIONS
- I THOUGHT I WAS DOING SOMETHING WRONG, UNTIL I REALIZED THAT…

BUGS, BUGS, BUGS…

RZCON 0x20 0x20

BUGS, BUGS, BUGS…

CVE-2020-12110 - TP-LINK CLOUD CAMERAS NCXXX HARDCODED ENCRYPTION KEY (3)

AFTER CHECKING ALL THE CODE, THERE WAS ONLY ONE THING LEFT TO CHECK…

github.com/VicoandMe/3DES/blob/master/des.h

```
static int IP_Table[64] = {  57,49,41,33,25,17,9,1,
                             59,51,43,35,27,19,11,3,
                             61,53,45,37,29,21,13,5,
                             63,55,47,39,31,23,15,7,
                             56,48,40,32,24,16,8,0,
                             58,50,42,34,26,18,10,2,
                             60,52,44,36,28,20,12,4,
                             62,54,46,38,30,22,14,6};
```

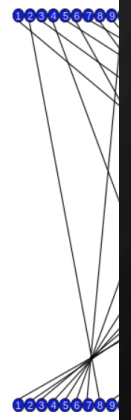
RANDOM TOOL ON THE INTERNET THAT SOMEHOW WORKS

en.wikipedia.org/wiki/DES_supplementary_material

Initial permutation (IP) [edit]

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

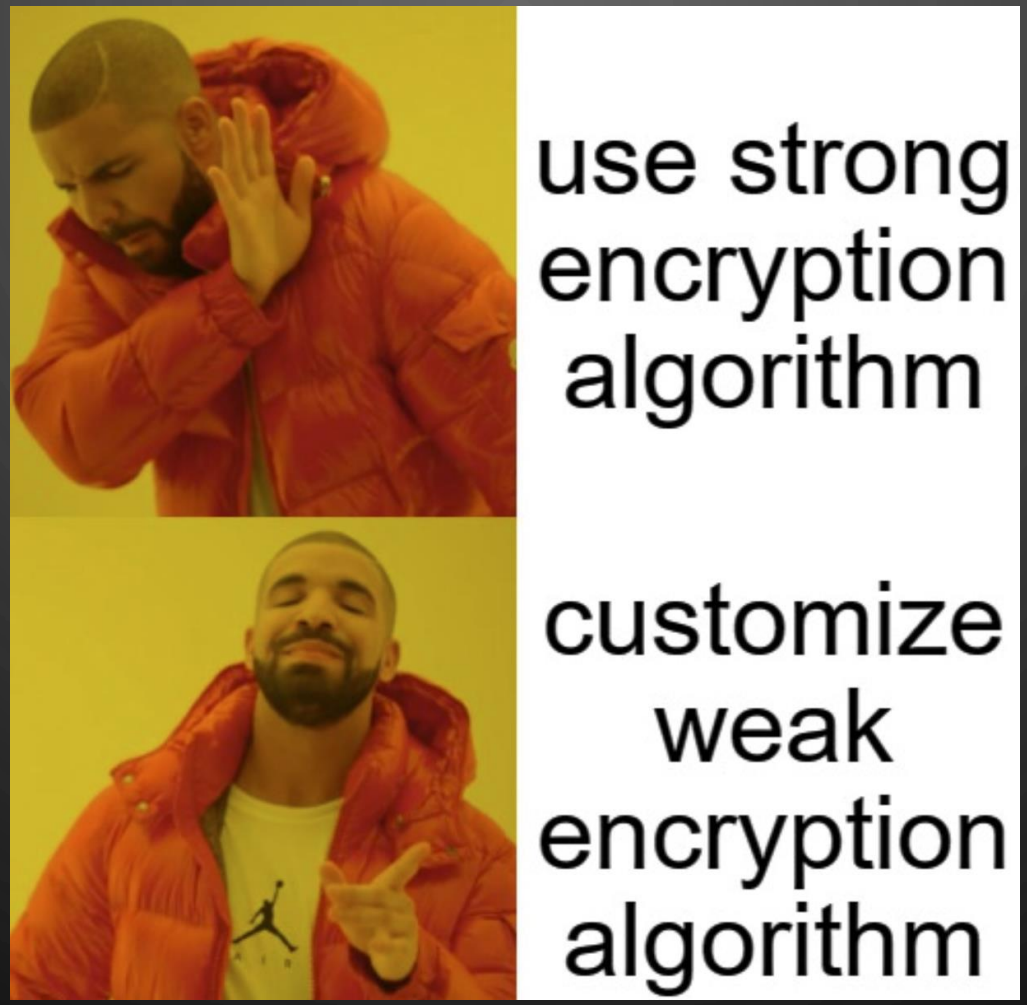


STANDARD DES

RZCON 2020

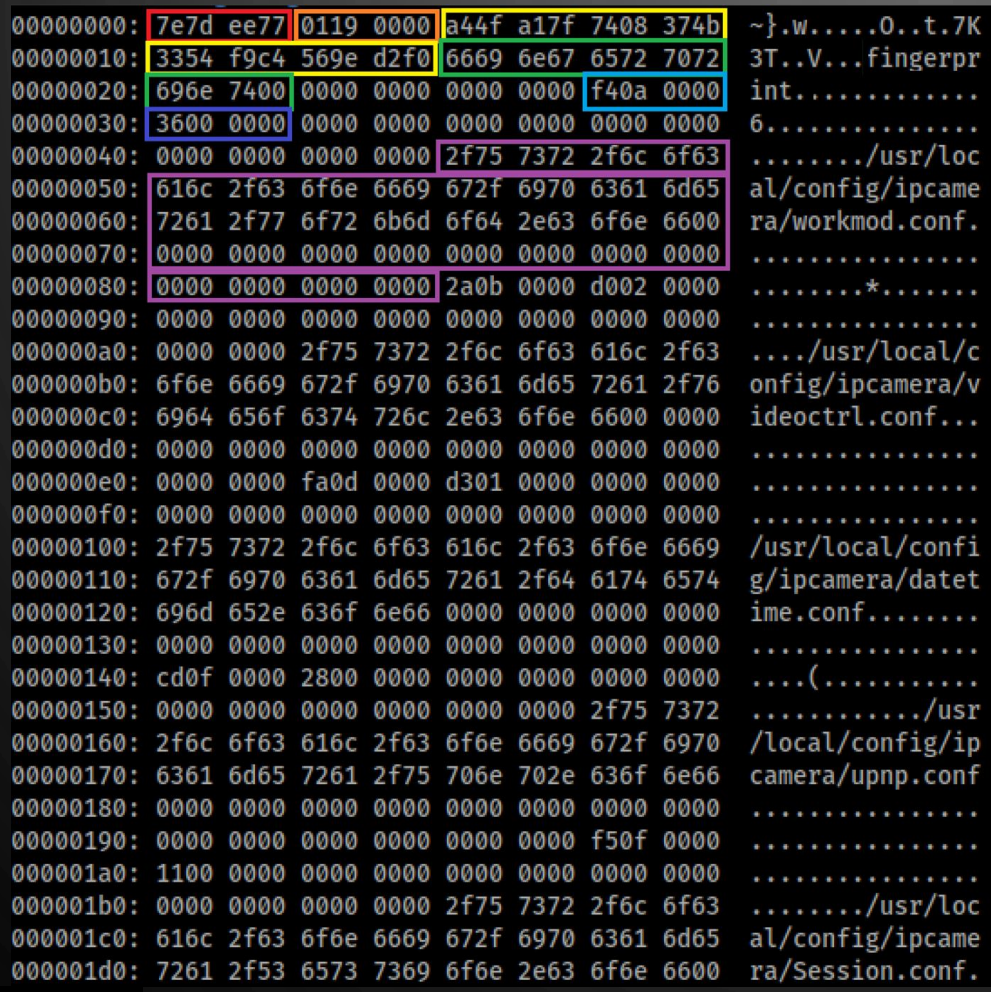
BUGS, BUGS, BUGS…

CVE-2020-12110 - TP-LINK CLOUD CAMERAS NCXXX HARDCODED ENCRYPTION KEY (4)



BUGS, BUGS, BUGS…

CVE-2020-12110 - TP-LINK CLOUD CAMERAS NCXXX HARDCODED ENCRYPTION KEY (5)



Header:

4 bytes: Magic

4 bytes: File size

16 bytes: File MD5

12 bytes: Null-terminated string "fingerprint"

8 bytes: Zero padding

File entries:

4 bytes: Absolute offset of file content

4 bytes: File size

20 bytes: Zero padding

64 bytes: Null-terminated file name + padding

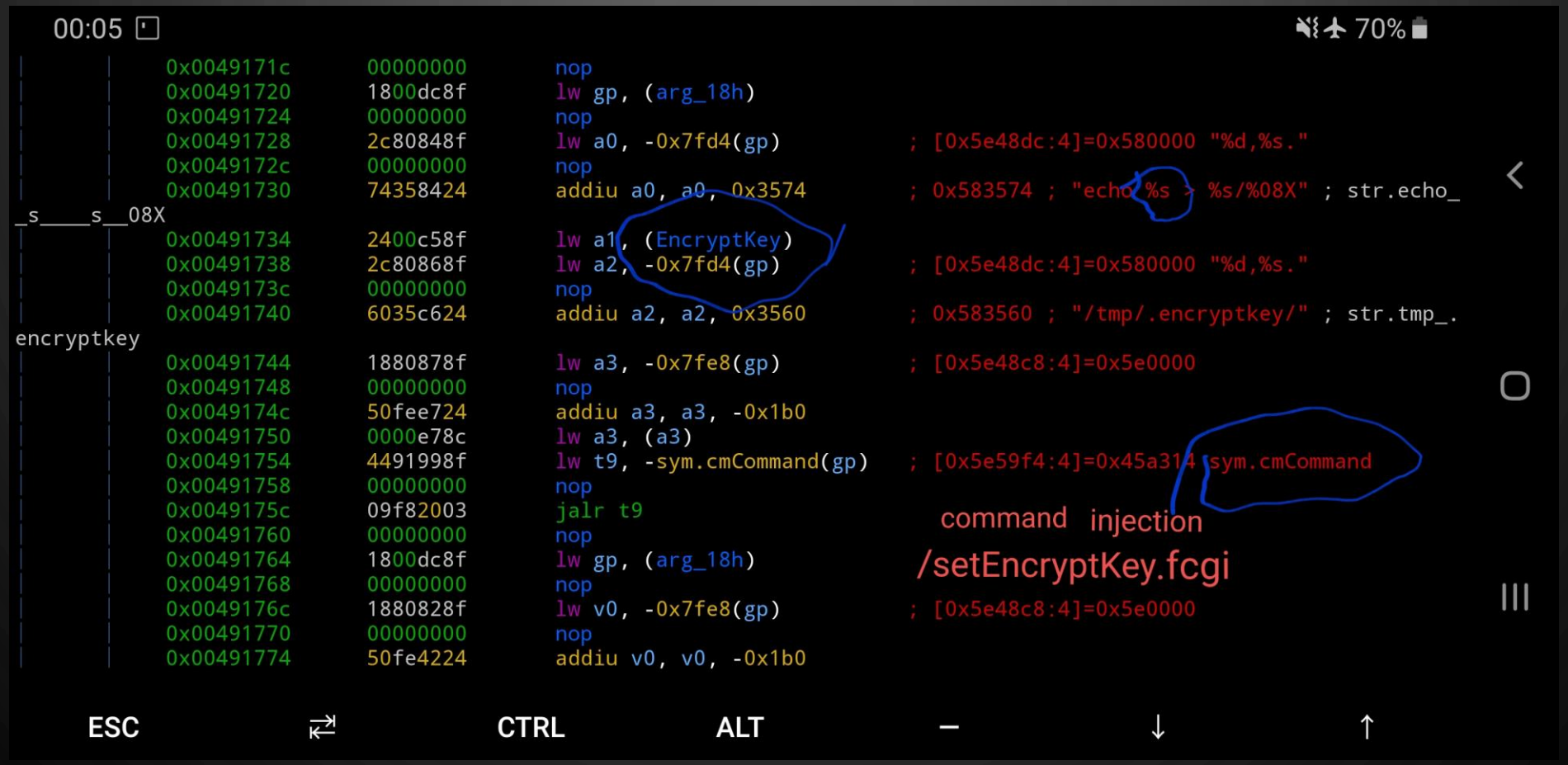
BUGS, BUGS, BUGS…

CVE-2020-12110 - TP-LINK CLOUD CAMERAS NCXXX HARDCODED ENCRYPTION KEY (6)

DEMO

BUGS, BUGS, BUGS…

CVE-2020-12111 - TP-LINK CLOUD CAMERAS NCXXX SETENCRYPTKEY COMMAND INJECTION



THIS ONLY AFFECTED NC260 AND NC450 CAMERAS

BUGS, BUGS, BUGS…

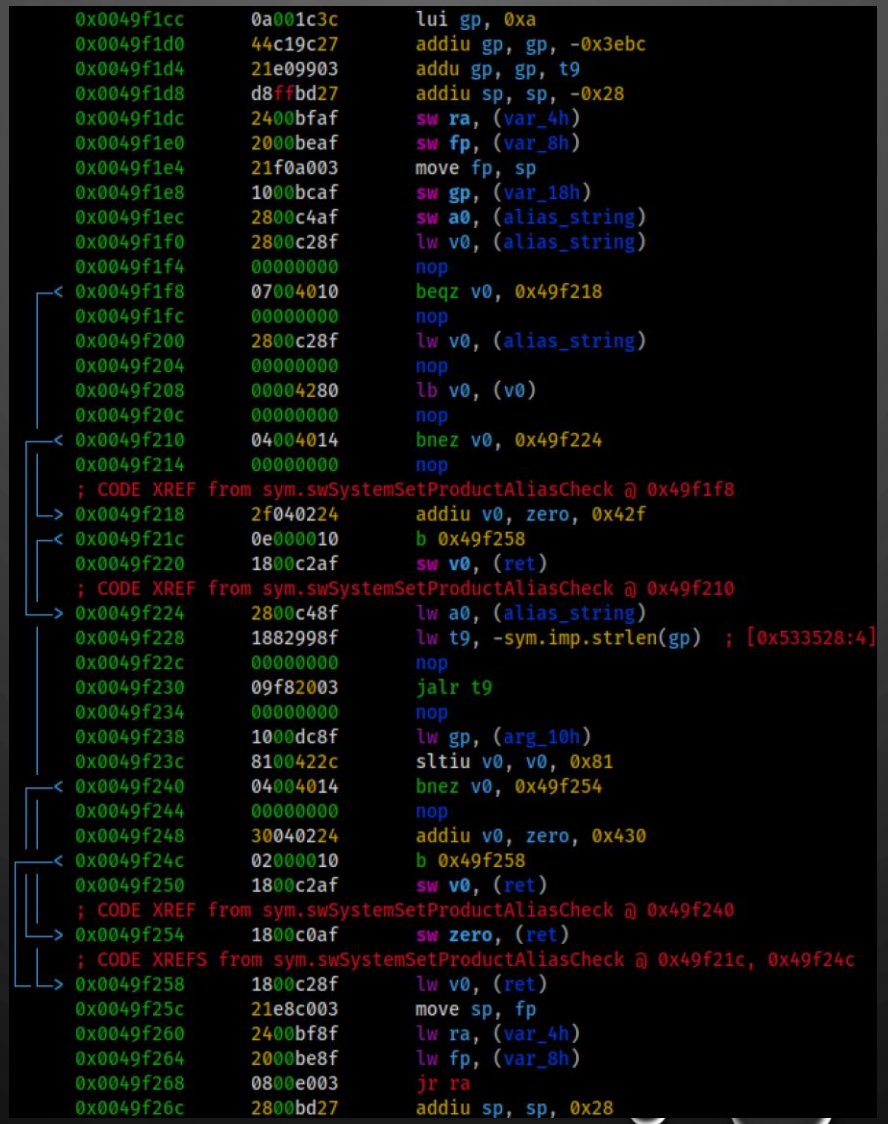
CVE-2020-12109 - TP-LINK CLOUD CAMERAS NCXXX BONJOUR COMMAND INJECTION (1)

```
    0x00439fc4      000d8424        addiu a0, a0, 0xd00         ; 0x4e0d00 ; "BONJOUR_STATUS" ; arg1 ; str.BONJOUR_STATUS
    0x00439fc8      6889998f        lw t9, -sym.sysConfGetLong(gp) ; [0x533c78:4]=0x432858 sym.sysConfGetLong ; "X(C"
    0x00439fcc      00000000        nop
    0x00439fd0      09f82003        jalr t9
    0x00439fd4      00000000        nop
    0x00439fd8      1000dc8f        lw gp, (arg_10h)
┌─< 0x00439fdc      1e004010        beqz v0, 0x43a058
│   0x00439fe0      00000000        nop
│   0x00439fe4      2000c227        addiu v0, fp, 0x20
│   0x00439fe8      21204000        move a0, v0
│   0x00439fec      21280000        move a1, zero
│   0x00439ff0      88000624        addiu a2, zero, 0x88        ; arg3
│   0x00439ff4      4887998f        lw t9, -sym.imp.memset(gp)  ; [0x533a58:4]=0x4dd5f0 sym.imp.memset
│   0x00439ff8      00000000        nop
│   0x00439ffc      09f82003        jalr t9
│   0x0043a000      00000000        nop
│   0x0043a004      1000dc8f        lw gp, (arg_10h)
│   0x0043a008      2000c227        addiu v0, fp, 0x20
│   0x0043a00c      21204000        move a0, v0
│   0x0043a010      88000524        addiu a1, zero, 0x88        ; arg2
│   0x0043a014      cc84998f        lw t9, -sym.swBonjourGetName(gp) ; [0x5337dc:4]=0x43a198 sym.swBonjourGetName
│   0x0043a018      00000000        nop
│   0x0043a01c      09f82003        jalr t9
│   0x0043a020      00000000        nop
│   0x0043a024      1000dc8f        lw gp, (arg_10h)
│   0x0043a028      2000c227        addiu v0, fp, 0x20
│   0x0043a02c      2480848f        lw a0, -0x7fdc(gp)          ; [0x533334:4]=0x4e0000
│   0x0043a030      00000000        nop
│   0x0043a034      100d8424        addiu a0, a0, 0xd10         ; 0x4e0d10 ; "mDNSResponderPosix -n \"%s\" -t _http._tcp -p %d -x path=/login.html &"
; str.mDNSResponderPosix__n___s___t__http._tcp__p__d__x_path__login.html
│   0x0043a038      21284000        move a1, v0
│   0x0043a03c      b000c68f        lw a2, (arg_b0h)
│   0x0043a040      a08b998f        lw t9, -sym.cmCommand(gp)   ; [0x533eb0:4]=0x449364 sym.cmCommand
```

SWBONJOURSTARTHTTP

BUGS, BUGS, BUGS…

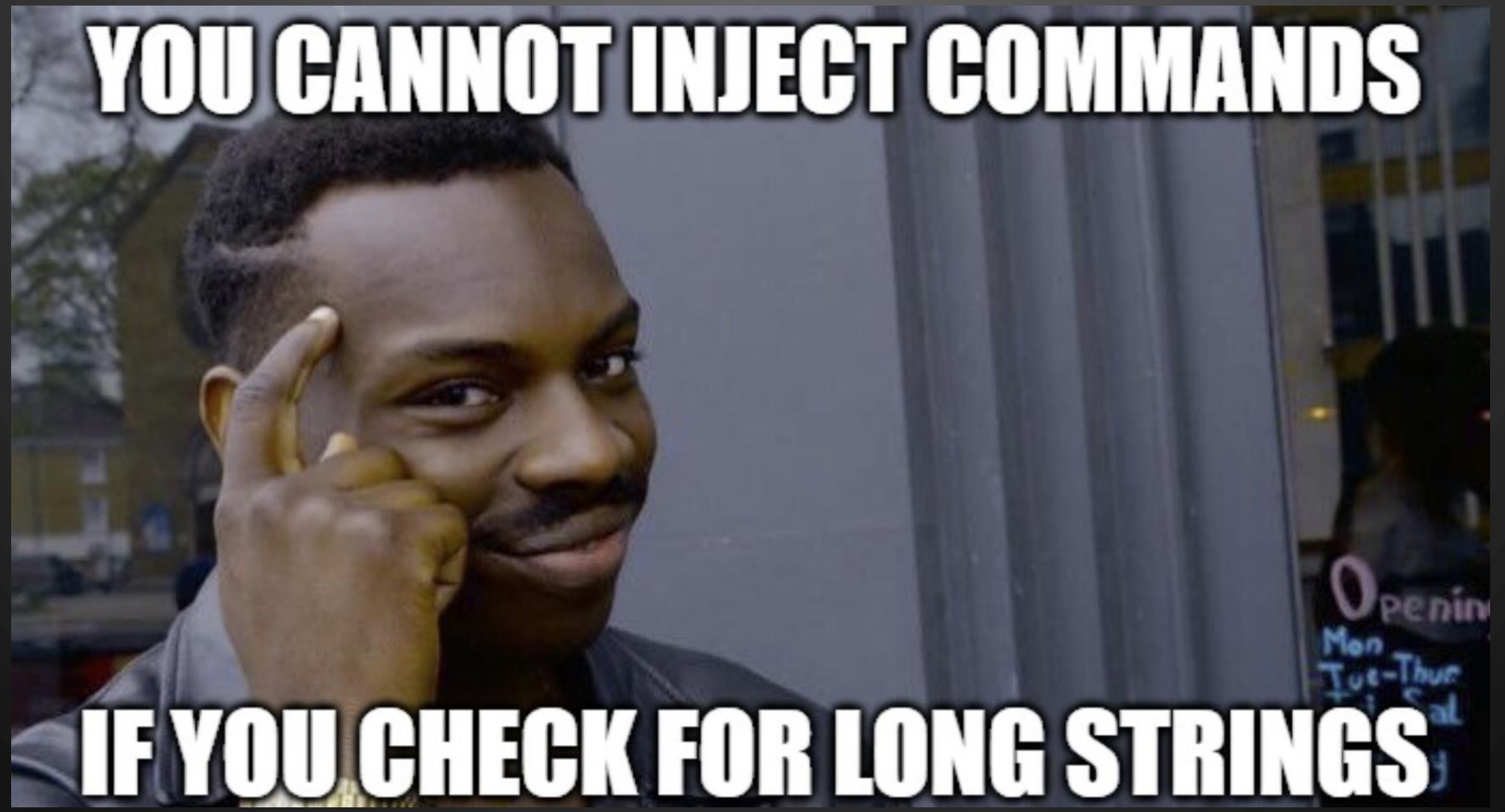
CVE-2020-12109 - TP-LINK CLOUD CAMERAS NCXXX BONJOUR COMMAND INJECTION (2)



SWSYSTEMSETPRODUCTALIASCHECK

BUGS, BUGS, BUGS…

CVE-2020-12109 - TP-LINK CLOUD CAMERAS NCXXX BONJOUR COMMAND INJECTION (3)



BUGS, BUGS, BUGS…

CVE-2020-12109 - TP-LINK Cloud Cameras NCXXX Bonjour Command Injection (4)

ONE BUG TO RULE THEM ALL:

- THIS BUG AFFECTED ALL 7 NC CAMERAS
- CAN BE TRIGGERED EASILY
- GIVES US EASY AND RELIABLE ROOT SHELL

BUGS, BUGS, BUGS…

CVE-2020-12109 - TP-LINK CLOUD CAMERAS NCXXX BONJOUR COMMAND INJECTION (5)

DEMO

LESSONS LEARNED

- CHECK VENDOR WEBSITE BEFORE DUMPING DEVICE FLASH
- CODE REUSE = SAME VULNERABILITIES ACROSS DIFFERENT DEVICES
- DROPPING A ZERO-DAY AFTER FIX DEADLINE HAS PASSED CAN GET THE VENDOR TO FIX ISSUES AND TAKE YOUR REPORTS SERIOUSLY
- REVERSE ENGINEERING CAN REVEAL BUGS THAT CANNOT BE FOUND VIA FUZZING/BLACK BOX TESTING

FUTURE WORK

LIST OF THINGS THAT WAS ORIGINALLY IN MY TODO LIST:

- LOOK FOR VULNERABILITIES THAT CAN BE EXPLOITED FROM TP-LINK CLOUD
- LOOK FOR VULNERABILITIES IN THE BROWSER PLUGIN
- LOOK FOR BASEBAND (WI-FI) VULNERABILITIES

CONCLUSIONS

- THERE WAS MORE THAN JUST ONE VULNERABILITY ON NC CAMERAS
- YOU DON'T NEED EXPENSIVE TOOLS TO FIND THOSE ISSUES
- IT IS POSSIBLE TO FIND ISSUES WITH A MOBILE PHONE ON A PLANE
- REVERSING IS NECESSARY TO COMPLEMENT FUZZING/BLACK BOX TESTING
- IT WAS A GOOD IDEA TO NEVER CONNECT MY CAMERA TO THE CLOUD
- I CAN NOW SAY FROM EXPERIENCE THAT SOME IOT DEVICES ARE INDEED INSECURE
- SECURITY RESEARCHERS AND VENDORS HAVE A SHARED RESPONSIBILITY AT MAKING THINGS MORE SECURE

THANK YOU FOR LISTENING

RZCON 2020