Bezpečnostná analýza domácich bezpečnostných kamier rodiny TP-Link Tapo

Bc. Jakub Šimo
Školiteľ: RNDr. Richard Ostertág, PhD.

31. august 2022

Fakulta matematiky, fyziky a informatiky
Univerzita Komenského v Bratislave

Inteligentná domácnosť - Smart Home

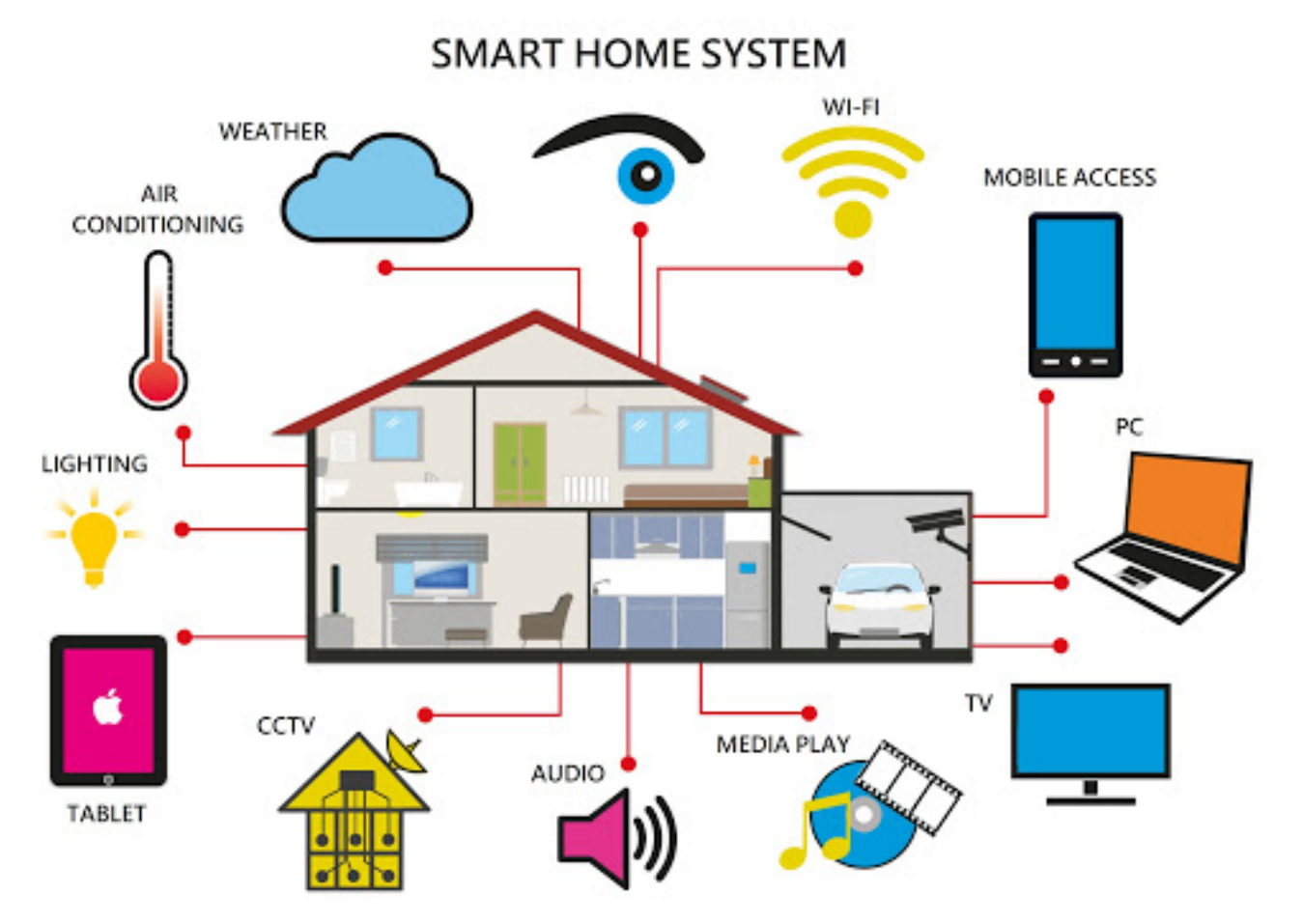


Image Source: http://visioforce.com/smarthome.html

Bezpečnostné IP kamery

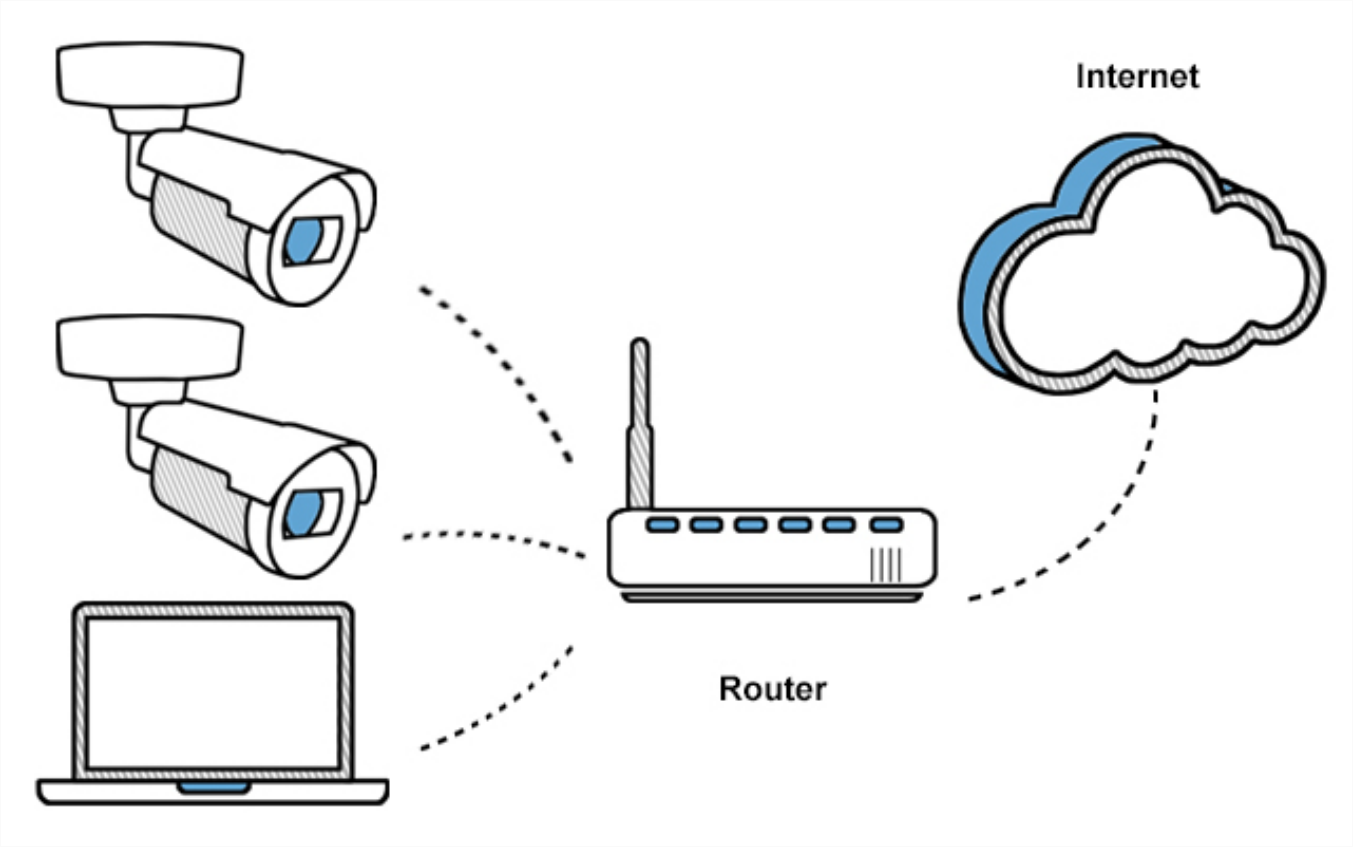


Image Source: https://touchit.sk/vsetko-co-potrebujete-vediet-o-ip-kamerach-tipy-na-zaujimave-zariadenia/323352

Objekty záujmu

Tapo C200 - jedna z najpredávanejších kamier v e-shope Alza

Rodina kamier Tapo - C100/C200/C310

Cieľ práce

- Preskúmať možnosti kompromitácie zariadenia

Image Source: https://www.dreamstime.com/stock-illustration-video-spy-bug-cartoon-icon-white-background-image79755251

Hardvér - vlastnosti

Motion Detection

Sound and Light Alarm

Night Vision

1080p Full HD

1080p Crystal Clear Image

Up to 128 GB (card not included)

Privacy Mode

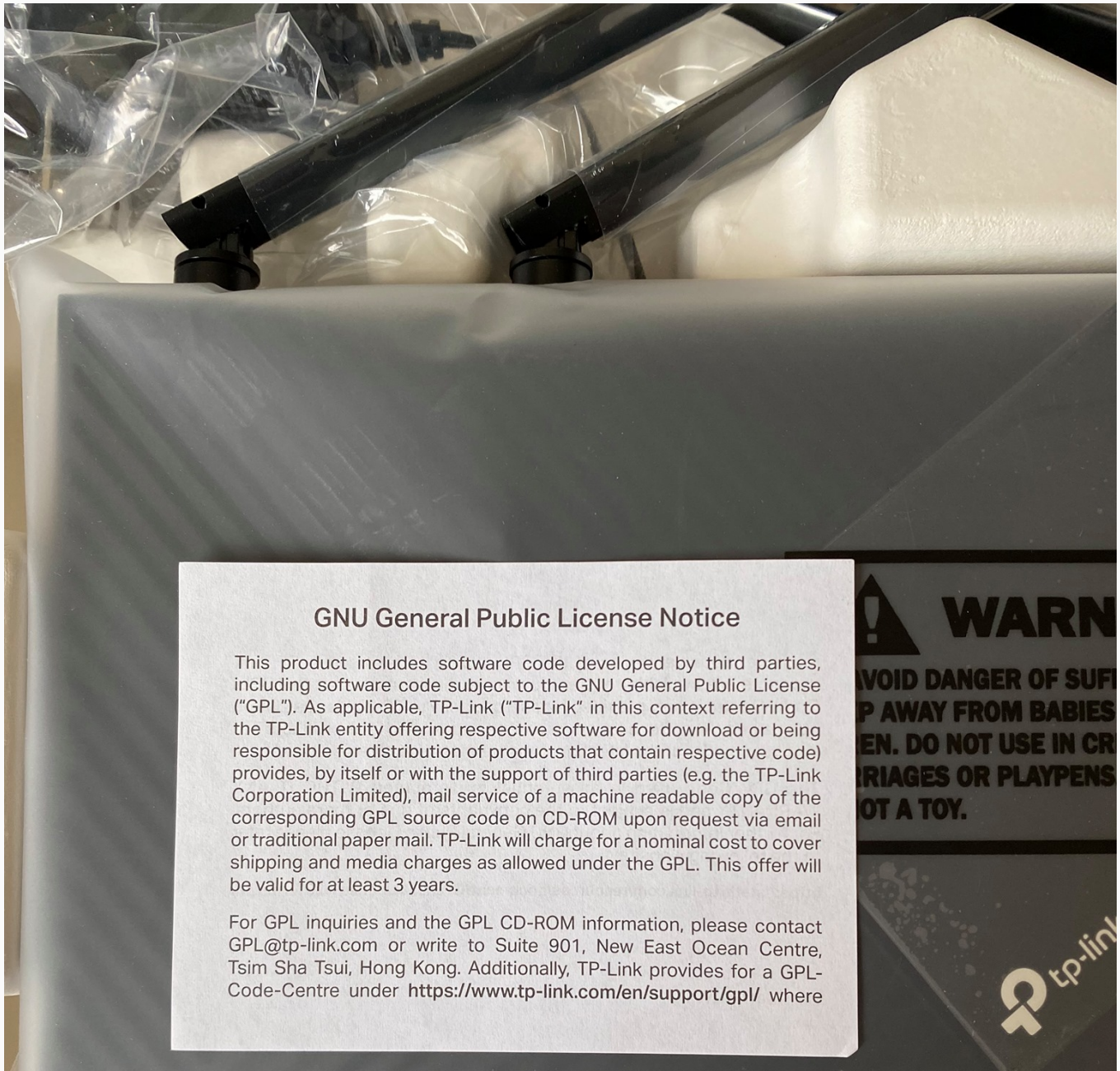
Doterajši výskum

- Lights, Camera, HACKED! An insight into the world of popular IP Cameras [1]

- pytapo knižnica
  - ovládanie niektorých funkcií podobne ako v mobilnej aplikacií (vyžaduje ale nastavenie v aplikacií)

[1] https://research.nccgroup.com/2020/07/31/lights-camera-hacked-an-insight-into-the-world-of-popular-ip-cameras/

Analýza - GPL zdrojový kód



Analýza - GPL zdrojový kód

Stáhnout pro Tapo C100 V1

Product Overview

Tapo C100(EU)_V1_Datasheet

Dokument

Tapo Camera(37Lanuages)_Quick Installation Guide
Tapo Camera(37languages)_V1_Quick Installation Guide
Tapo C100(EU)_V1_User Guide
Tapo C100(EU)_V1_Quick Installation Guide

Domácí bezpečnostní Wi-Fi kamera
Tapo C100

Setup Video | Nejčastější dotazy | Apps | GPL Code

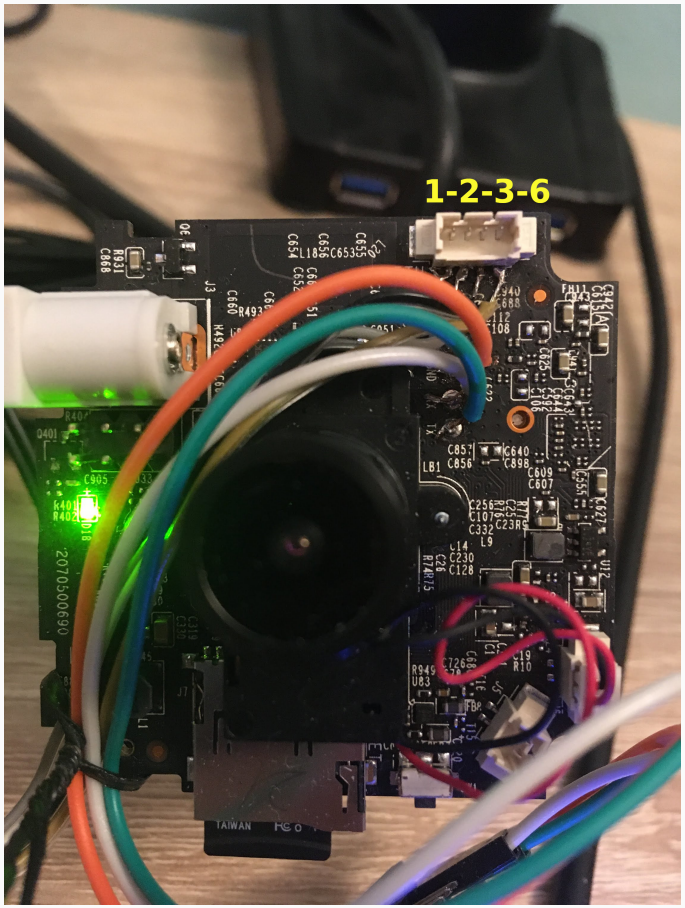
GPL Code

Tapo C100(EU)_V1_GPL

Analýza - GPL zdrojový kód

```
1 $ cat etc/openwrt_release
2 DISTRIB_ID="OpenWrt"
3 DISTRIB_RELEASE="Attitude␣Adjustment"
4 DISTRIB_REVISION="41bbac3d1dba36d21943edf2f2716c0476ab006a"
5 DISTRIB_CODENAME="attitude_adjustment"
6 DISTRIB_TARGET="realtek/generic"
7 DISTRIB_DESCRIPTION="OpenWrt␣Attitude␣Adjustment␣12.09-rc1"
```

Analýza - sériová konzola



Kamera s pripojeným UART a vyznačením Ethernet pripojením

Analýza - sériová konzola

```
$ cat logs/screenlog.0
U-Boot 2014.01-v1.2 (Nov 08 2019 - 09:07:14)
Board: IPCAM RTS3903 CPU: 500M :rx5281 prid=0xdc02
<... ommited lines ...>
verifying uboot partition...
ok
verifying kernel and romfs partition...
ok
set watchdog, resetting...

U-Boot 2014.01-v1.2 (May 19 2020 - 18:26:56)
Board: IPCAM RTS3903 CPU: 500M :rx5281 prid=0xdc02
<... the log goes on ...>
```

Začiatok výstupu z bootlogu zariadenia

Analýza - sériová konzola

```
442 $ less gpl-code/c100_GPL_v1/torchlight/product_config/ALL/buildroot.config
443 # CONFIG_USE_MKLIBS is not set
444 CONFIG_USE_UCLIBCXX=y
445 # CONFIG_USE_LIBSTDCXX is not set
446
447 #
448 # SLP global settings
449 #
450 CONFIG_SLP_LOGIN_PASSWORD="slprealtek"
451 CONFIG_DEVEL=y
452 # CONFIG_BROKEN is not set
453 CONFIG_DOWNLOAD_FOLDER=""
```

Heslo v zdrojovom kóde

Analýza - sériová konzola

```
May 19 12:34:11 login[1155]: root login on 'ttyS1'

BusyBox v1.19.4 (2020-05-19 18:22:58 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

   SSSSSSSSSSSSSSS      LLLLLLLLLLLLL              PPPPPPPPPPPPPPPPPPPP
  SSSSSSSSSSSSSSSSS      LLLLLLLLLLLLL              PPPPPPPPPPPPPPPPPPPPPPP
SSSSSS        SSSSSSSS        LLLLLL                    PPPPPP        PPPPPPPP
SSSSSS          SSSSSS        LLLLLL                    PPPPPP          PPPPPP
SSSSSSSS          SSSS        LLLLLL                    PPPPPP          PPPPPP
  SSSSSSSSSSSSSS              LLLLLL                    PPPPPP        PPPPPPPP
    SSSSSSSSSSSSSSS           LLLLLL                    PPPPPPPPPPPPPPPPPPP
       SSSSSSSSSSSSS          LLLLLL                    PPPPPPPPPPPPPPPP
SSSS          SSSSSSSSS      LLLLLL          LL        PPPPPP
SSSSSS            SSSSSS     LLLLLL        LLLLLL      PPPPPP
SSSSSSSS          SSSSSS     LLLLLL        LLLL        PPPPPP
  SSSSSSSS      SSSSSSSS     LLLLLL      LLLLLLLL      PPPPPP
  SSSSSSSSSSSSSSSSSS    LLLLLLLLLLLLLLLLLLLLLLL    PPPPPPPPPPPPP
  SSSS  SSSSSSSSS       LLLLLLLLLLLLLLLLLLLLL      PPPPPPPPPPPPP
--------------------------------------------------------------------------------
SMARTs, the power to be your best! (torchlight: svn <hash>)
--------------------------------------------------------------------------------
root@SLP:~#
```

Konzola po prihlásení

Zistenia - uloženie konfigurácie

```
1 DES_Decrypt(
2   "/tmp/config.bin",
3   "jklsd*%&%HDFG767",
4   "/tmp/decrypt_conf"
5 );
```

Kód dešifrujúci konfiguráciu

Firmvér

Stáhnout pro Archer C7 V5

Prosím zvolte si hardwarovou verzi:

V5

> Jak zjisti hardwarovou verzi vašeho TP-Link zařízení?

Modely a hardwarové verze se liší v závisloti na regionu. Prosím ujistěte se o detailech pokud zvažujete nákup.

Bezdrátový gigabitový router s duálním pásmem AC1750
Archer C7

Product Overview

Archer C7(EU)_V5_Datasheet

Dokument

SOHO Wireless Routers(EU2-16Languages)_ Quick Installation Guide
Archer C7(EU)_V5_User Guide
Archer C7(EU)_V5_Quick Installation Guide

Nástroj | Setup Video | Nejčastější dotazy | Firmware | Apps

GPL Code | Emulátory

Stránka TP-Link routeru poskytujúca firmvér

Firmvér

Stáhnout pro Tapo C100 V1

Product Overview

Tapo C100(EU)_V1_Datasheet

Dokument

Tapo Camera(37Lanuages)_Quick Installation Guide
Tapo Camera(37languages)_V1_Quick Installation Guide
Tapo C100(EU)_V1_User Guide
Tapo C100(EU)_V1_Quick Installation Guide

Domácí bezpečnostní Wi-Fi kamera
Tapo C100

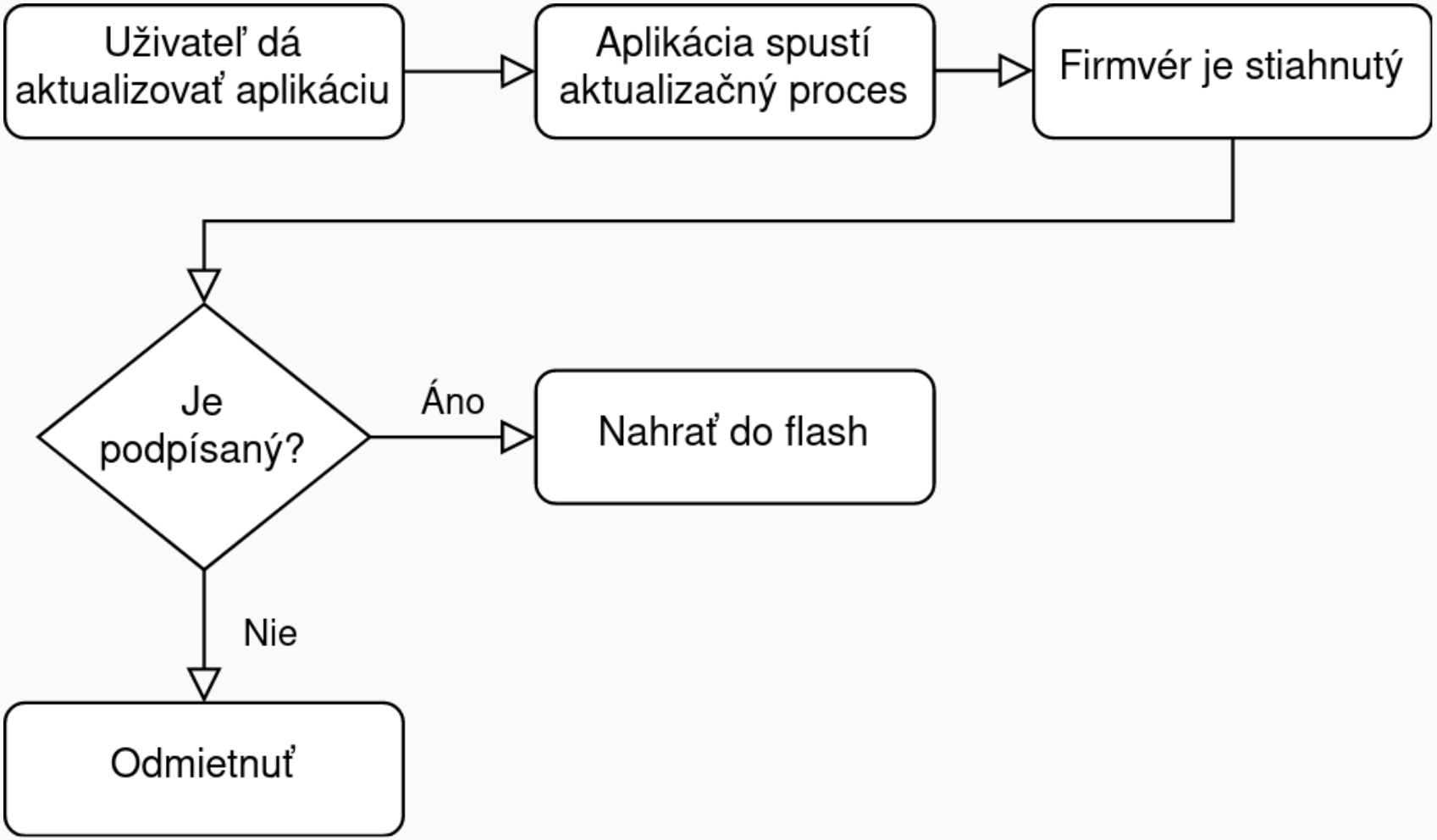
Setup Video | Nejčastější dotazy | Apps | GPL Code

GPL Code

Tapo C100(EU)_V1_GPL

Stránka kamery neposkytujúca firmvér

Firmvér - proces aktualizácie



Proces aktualizácie

Firmvér - aktualizácia

```
31      iVar1 = FUN_0040d820(param_1,"/tmp/firmware.img",local_16b0);
32      if (-1 < iVar1) {
33        func_0x00411760(auStack1568,0,0x401);
34        pcVar4 = "/tmp/.sysupgrade_result";
35        FUN_004116f0(auStack1568,0x401,"/sbin/slpupgrade -c %s > /dev/null 2>&1;echo $? > %s",
36                     "/tmp/firmware.img","/tmp/.sysupgrade_result");
37        iVar1 = FUN_0040d750(auStack1568,"/tmp/.sysupgrade_result");
38        if (iVar1 == -1) {
39          iVar1 = -0x9ca6;
40        }
41        else {
42          if ((iVar1 == 0) || (iVar1 = -0xc6d7 - iVar1, iVar1 == 0)) {
43            func_0x00411760(auStack1568,0,0x401);
44            FUN_004116f0(auStack1568,0x401,"fw forbid; sleep 1; /sbin/slpupgrade %s;",
45                         "/tmp/firmware.img",pcVar4);
```

Spustenie aktualizácie systému (Ghidra - uhttpd)

Firmvér - slpupgrade

```
004150c7 00              ??         00h

                     DAT_004150c8                                    XREF[1]:     main:
004150c8 12              ??         12h
004150c9 34              ??         34h    4
004150ca 56              ??         56h    V
004150cb 78              ??         78h    x

                     s_BgIAAACkAABSU0ExAAQAAAEAAQArjNXu_004150cc      XREF[2]:     main:
                                                                                  main:
004150cc 42 67 49        ds         "BgIAAACkAABSU0ExAAQAAAEAAQArjNXuvBeCGfOD19AGJ..."
         41 41 41
         43 6b 41 ...
```

Verejná časť RSA kľúča použitého na podpis aktualizácie
(Ghidra - slpupgrade)

Firmvér - slpupgrade

```
$ base64 -d /tmp/tplink.key.b64
$ openssl rsa -pubin -inform MS\ PUBLICKEYBLOB -in /tmp/tplink.key -outform PEM
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCcy5y1JQ+QqOf5p8HyZYXdMj1a
enr3AXfAbuNzD86DaMPjsP4Jp34sutCfjqnnuvng4cej9YoF/0mrhrVZ9IrOnYIQ
3J0D7KCarOx8fidlTSo2MOMDy/S/AJzN2d/6ZJi1K5hsNHk4rC/ou5Wnom95nGkk
BtDXg/MZghe87tWMKwIDAQAB
-----END PUBLIC KEY-----
```

PEM forma kľúča

Firmvér - slpupgrade

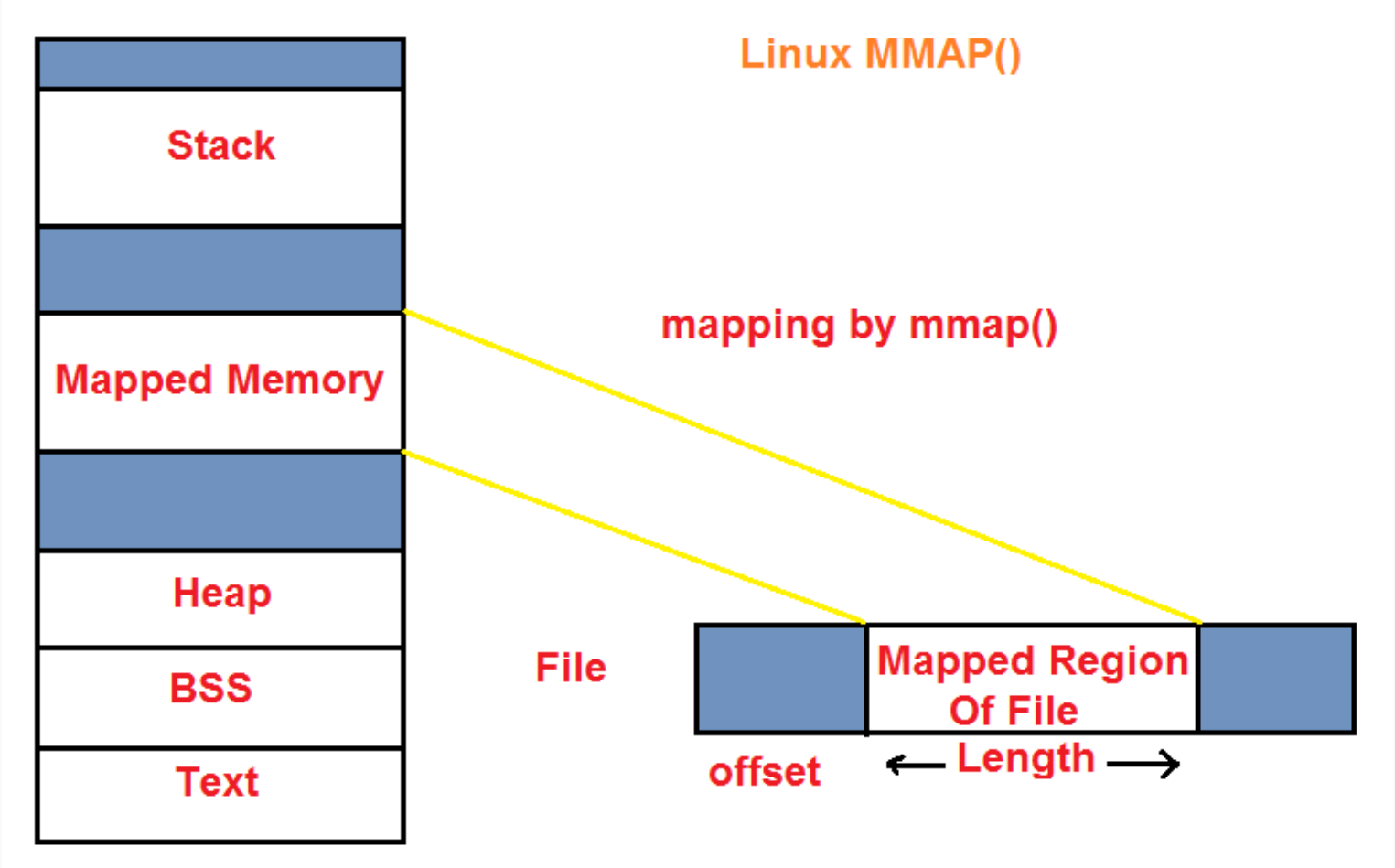


Image Source:
https://www.tutorialsdaddy.com/linux-device-drivers/introduction-to-linux/

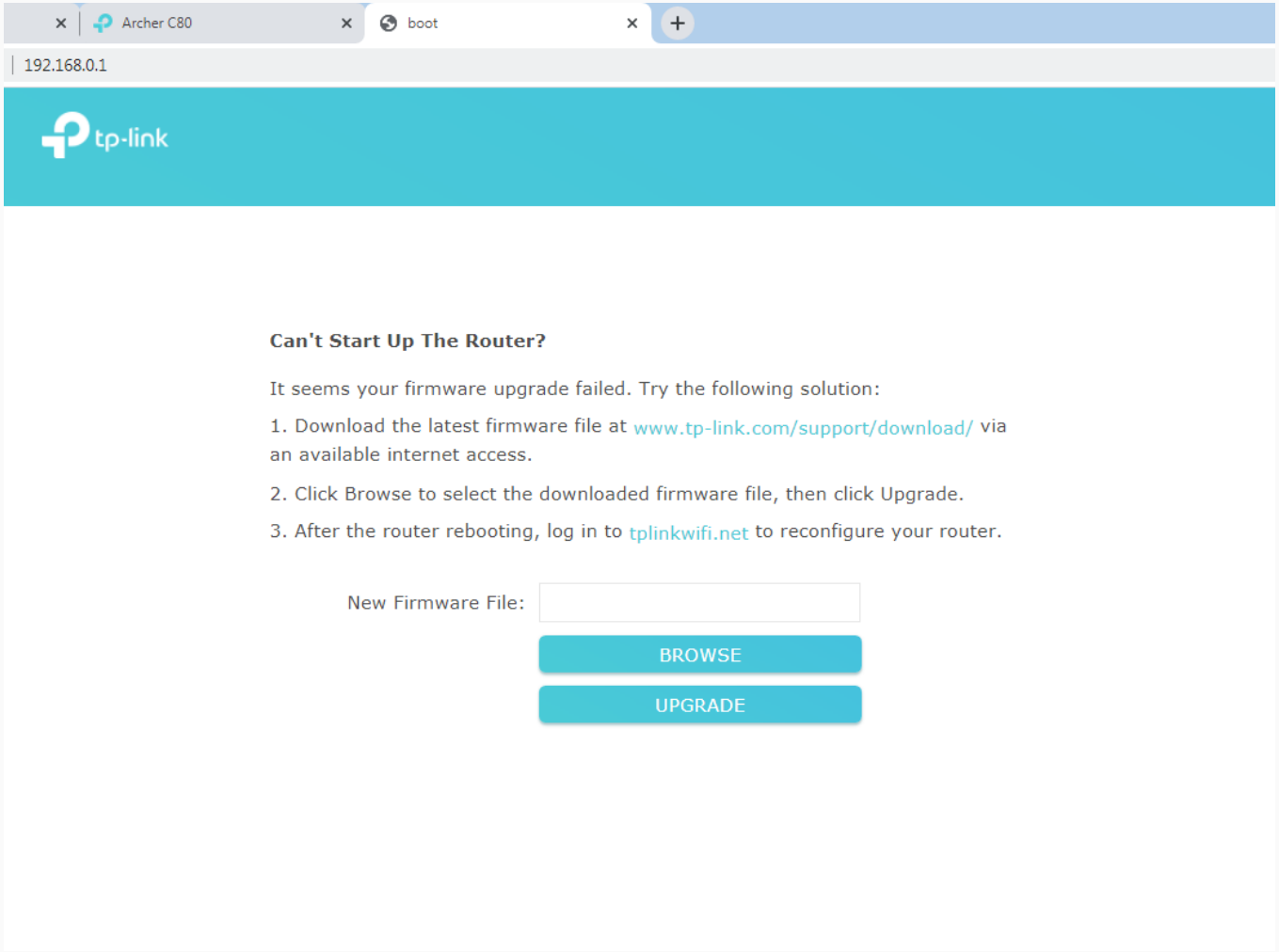
Firmvér - slpupgrade

```
$ xxd -c16 mtdblock8.img
00000000: 0000 0100 55aa 9dd1 a8c8 8331 c969 fbbf  ....U......1.i..
00000010: bcf0 d432 70c7 aa55 8001 0000 8030 8e70  ...2p..U.....0.p
00000020: 0000 0000 0000 0009 0000 0000 0001 d800  ................
00000030: 0001 d800 0000 2800 0002 0000 0002 0000  ......(.........
00000040: 0004 0000 0001 0000 0005 0000 0001 0000  ................
00000050: 0006 0000 0000 0200 0006 0200 0016 5e00  ..............^.
00000060: 001c 6000 0052 a000 006f 0000 0011 0000  ..`..R...o......
00000070: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000080: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000090: f604 99e7 5ebd 01bc 63fb ccdd ed59 a009  ....^...c....Y..
000000a0: b278 a964 23a7 ac43 b6f0 fa64 71cb 3364  .x.d#..C...dq.3d
000000b0: 8062 2c92 7d9c 28d4 324d dda1 308a 32f0  .b,.}.(.2M..0.2.
000000c0: 4331 3030 2031 2e30 0000 0000 0000 0000  C100 1.0........

$ dd if=mtdblock8.img bs=1 skip=512 count=6880768 | md5sum
6880768+0 records in
6880768+0 records out
6880768 bytes (6.9 MB, 6.6 MiB) copied, 3.62115 s, 1.9 MB/s
b278a96423a7ac43b6f0fa6471cb3364  -
```

Porovnanie kontrolného súčtu firmvéru

Firmvér - slpupgrade



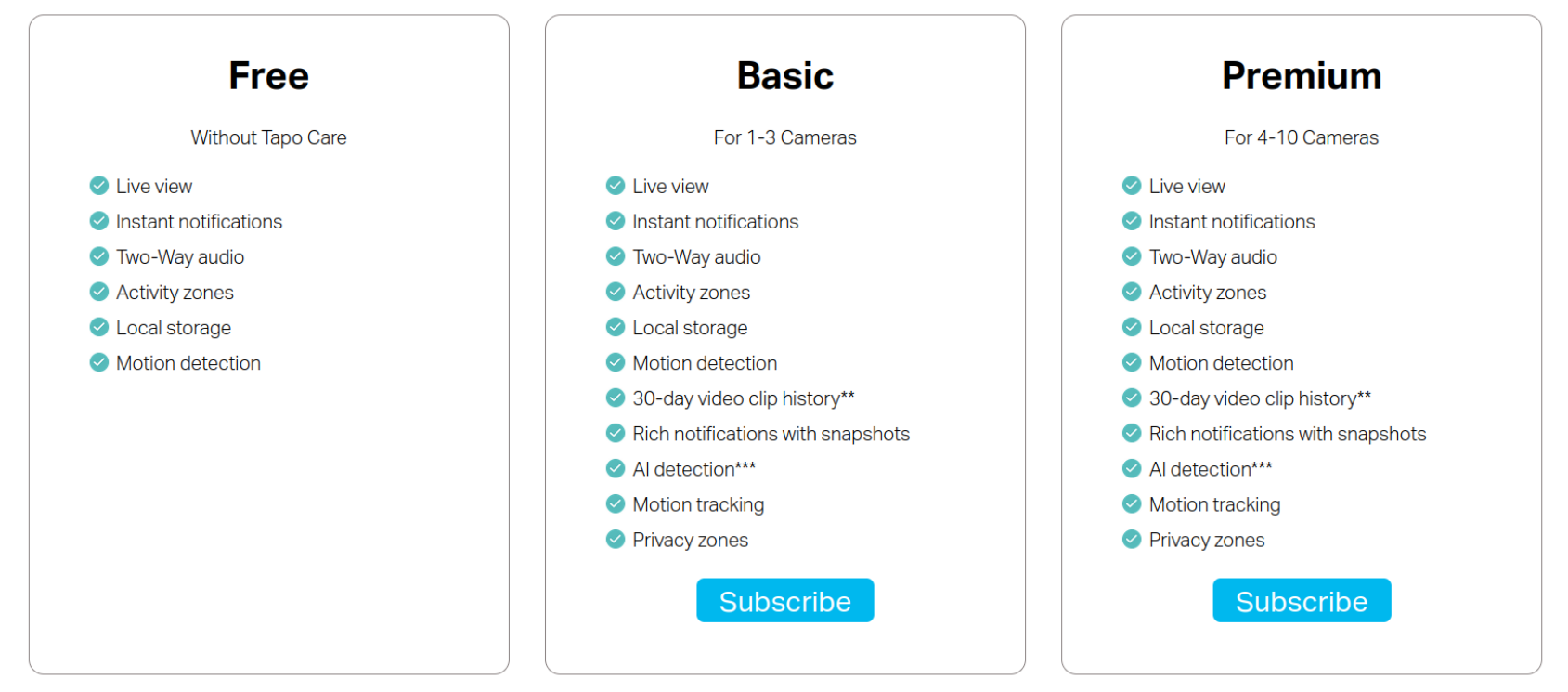
Ukážka záchranného módu router-u

Firmvér - check_upgrade skript

```
4  $ cat firmware/squashfs-root-1.0/etc/init.d/check_upgrade
5  start() {
6          if [ ! -d "/tmp/sdcard" ]; then
7                  mkdir -p /tmp/sdcard/
8          fi
9
10         if [ -b /dev/mmcblk0p1 ]; then
11                 mount -t vfat /dev/mmcblk0p1 /tmp/sdcard/
12         else
13                 exit 0
14         fi
15         echo "check␣firmware␣upgrade"
16         if [ -e /tmp/sdcard/factory_up_boot.bin ]
17         then
18                 echo "start␣firmware␣upgrade␣..."
19                 slpupgrade -n "/tmp/sdcard/factory_up_boot.bin"
20
21                 while true
22                 do
23                         sleep 10
24                 done
25         else
26                 umount /tmp/sdcard
27         fi
28 }
```

Skript kontrolujúci aktualizácie z SD karty pri spustení

Firmvér - novšie verzie



Úrovne ponuky Tapo Care

uhttpd komunikácia

```
96  $ cat firmware/squashfs-root-1.0/etc/init.d/uhttpd
97  config_get https "$cfg" listen_https
98  config_get UHTTPD_KEY  "$cfg" key  /etc/uhttpd.key
99  config_get UHTTPD_CERT "$cfg" cert /etc/uhttpd.crt
100 [ -n "$https" ] && {
101         [ -f "$UHTTPD_CERT" -a -f "$UHTTPD_KEY" ] || {
102                 config_foreach generate_keys cert
103         }
104         [ -f "$UHTTPD_CERT" -a -f "$UHTTPD_KEY" ] && {
105                 append_arg "$cfg" cert "-C"
106                 append_arg "$cfg" key  "-K"
107                 for listen in $https; do
108                         append UHTTPD_ARGS "-s␣$listen"
109                 done
110         }
111 }
```

Konfigurácia uhttpd

uhttpd komunikácia

```
$ cat logs/setup/protocol/formatted/1-auth.log
POST / HTTP/1.1
<... headers ...>

{
  "method": "login",
  "params": {
    "hashed": true,
    // this is just md5sum of "admin"
    "password": "21232F297A57A5A743894A0E4A801FC3",
    "username": "admin"
  }
}

-----------------------------------------------------------------------
HTTP/1.1 200 OK
<... headers ...>

{
  "error_code": 0,
  "result": {
    "stok": "a0a1251ed3ff1be92977b8b86c2eb4b5",
    "user_group": "root"
  }
}
```

Príklad dešifrovanej komunikácie - autorizačné volanie

Výsledky

- Dešifrovali sme celú komunikáciu zariadenia s aplikáciou
- Vieme downgradeovať systém zariadenia
- Vieme pri soft-bricku zariadenie obnoviť do pôvodného stavu
- Vieme perzistentne upraviť firmvér zariadenia
    - CVE skóre podľa oficiálnej kalkulačky okolo 7

Výsledky spolupráce

Hacefresko All Posts Posts by Tag Terms

Hacefresko

Computer science student interested in cybersecurity

Twitter

Github

HackerOne

TP-Link Tapo c200 Unauthenticated RCE

17 minute read

Published: February 11, 2022

Hello there. Today I would like to share with you my first CVE, which corresponds to a command injection vulnerability found a couple months ago in the TP-Link Tapo c200 camera, that allows an attacker to take full control of the device with root privileges. It was assigned CVE-2021-4045 by the INCIBE, and you can check the official advisory here. The vulnerability affects all firmware versions prior to 1.1.16 Build 211209 Rel. 37726N, so if you own this model, I suggest you update it.

Stránka oznamujúca RCE zraniteľnosť

Oznámenie nedostatkov výrobcovi

- poznatky sme oznámili výrobcovi cez dezignovaný kanál
- výrobca prijal náš oznam
- od 10. júna "vyhodnocujú"

Ďaľšia práca

- kontrola novších verzií a revízií
  - novšie kamery používajú štandardný ARM SoC
- pridanie funkcionality do firmvéru - zálohovanie videí je obľúbená žiadosť

Záver

- dobrý hardvér za cenu
- pre bezpečné používanie treba mať know-how

Otázky?

Ďakujem za pozornosť

Posudok - školitel - Elektronická príloha

- Otázka: Aký zmysel má v prílohe adresár tmp?
- Odpoveď: Nachádzajú sa v ňom rozobraté firmware-y v rôznom stave úpravy, pôvodne som chcel referovať na rôzne kroky repackovania.

Posudok - oponent - Navrhnuté riešenie

- "Napriek pokusu o modifikáciu firmvéru študent nedokázal modifikovať firmvér tak, aby potvrdil zraniteľnosť."
  - strana 26-27
  - "Since we now know the offsets, we can recalculate the checksums after changing parts of the firmware."
  - " With our acquired know-how, we were able to modify the firmware and change the service file so that telnet would accept all connections."
  - áno, v texte chýba viac konkrétnych príkladov na ilustráciu

Posudok - oponent - Formálna stránka

- "Práca s literatúrou je na slabej úrovni, málo vedeckých zdrojov."
    - áno, zdroje sú z väčšiny webové, no v tejto sfére sú výsledky zverejnované skôr vo forme blogov/prezentácií (napr. DEFCON)

Posudok - oponent - Formálna stránka

Index of Tapo camera thesis

Citation websites

You can click on the links to open locally saved versions of the websites, as accessed at the time of writing.

1. The High Cost of Wasted Printer Ink - Consumer Reports
2. Discussion regarding the camera on github
3. DrSamnoLiu Blog - The Tapo C200 Research Project.
4. TP-Link Tapo c200 Unauthenticated RCE - Hacefresko
6. New Progress in China's Protection of Intellectual Property Rights
7. TP-Link firmware layout
8. NIST CVSS Calculator
9. Lights, Camera, HACKED! An insight into the world of popular IP Cameras - NCC Group Research
10. Lexra insider story
11. Press statement about Tapo spin-off
12. Tapo Care landing page
13. TP-Link ranks as World's No.1 Wi-Fi Products Provider for 10 Years
14. TP-Link firmware header layout

Rozcestník v prílohe