

Jak szukać podatności i zgłaszać błędy producentom urządzeń IoT - case study

Artur „Lucky” Łącki

Poznań Security Meetup - #2 2024

\$ whoami

- Kiedyś tester w dziale QA
- Od 2017 roku Inżynier Systemów Wbudowanych
- Gościnnie gram w CTFy z justCatTheFish
 - <https://justcatthefish.team/>
- alacki93@gmail.com
- lackylab.pl

Agenda

- Potrzebna wiedza i narzędzia
- Wybór urządzenia
- Środowisko testowe
- Rekonesans
- Uzyskanie dostępu do oprogramowania
- Na co patrzeć, czyli częste błędy w świecie IoT
- Zgłaszamy błąd

Wiedza i narzędzia

- **BHP przy pracy z prądem elektrycznym**
- Podstawy elektrotechniki i elektroniki
 - Kurs elektroniki od podstaw – Forbot
 - Podstawowe standardy komunikacji: UART, SPI, 1wire, I2C
 - Podstawy posługiwania się multimetrem
- Znajomość architektury CPU urządzenia

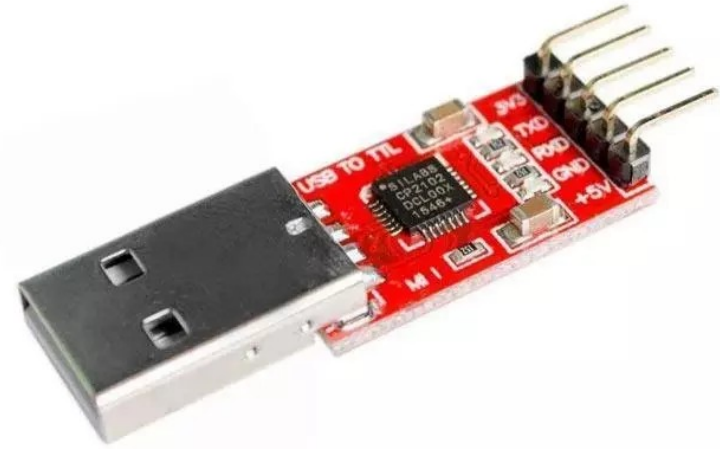
- Zestaw precyzyjnych śrubokrętów i narzędzia do otwierania obudów



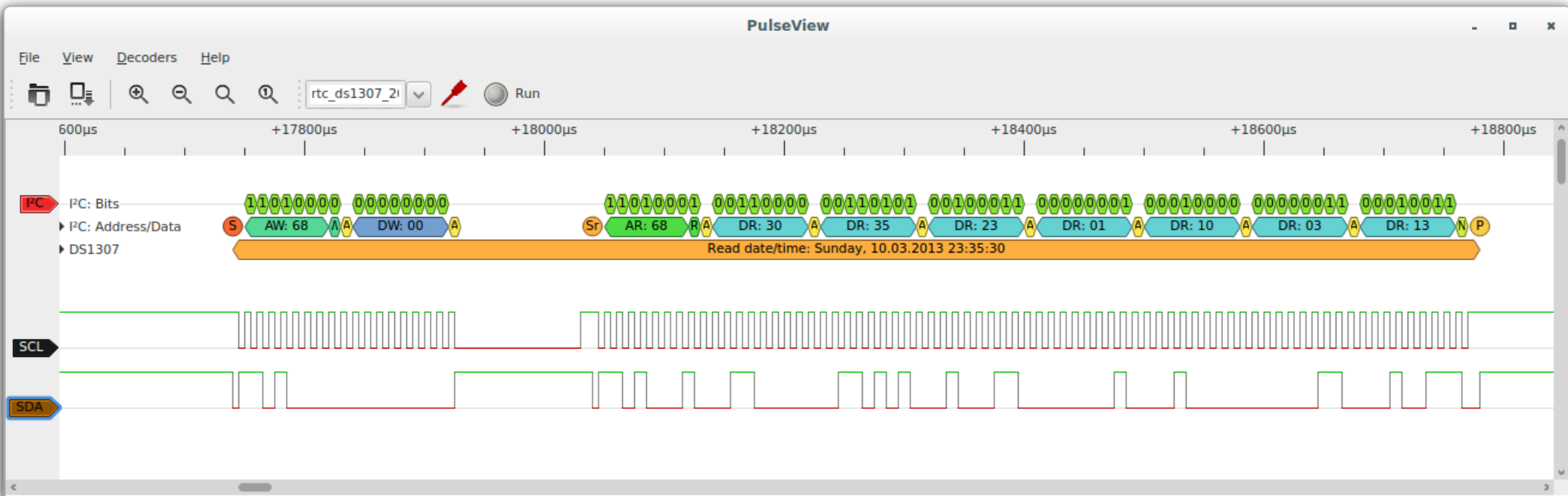
- Multimetr
 - Woltomierz
 - Amperomierz
 - Omomierz
 - Tester ciągłości obwodu/
wykrywacz zwarć/brzęczyk



- Przejściówka USB-UART
 - Po podłączeniu widoczne jako /dev/ttyUSBx (Linux) lub COMx (Windows)



- Analizator stanów logicznych
 - https://sigrok.org/wiki/Supported_hardware
 - Saleae (i klony)



Wybór urządzenia

- Budżet
- Powierzchnia ataku
- Dostęp do firmware
- Kontakt z producentem



Rekonesans

- Czytamy instrukcję obsługi!
- Podłączamy urządzenie przez środowisko testowe i monitorujemy ruch
- Poznajemy funkcje urządzenia
- Skanujemy porty
- Rozbieramy urządzenie i patrzymy co jest w środku

Środowisko testowe

Telefon z systemem Android



Połączenie Wi-Fi
Podsieć 10.42.0.0/24

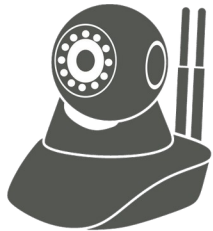
Komputer z systemem Linuks



Serwery chmury producenta:
app.example.com
p2p1.example.com
p2p2.example.com



Połączenie z internetem



Kamera IP

Połączenie Ethernet
Podsieć 10.42.1.0/24

Rekonesans

Nmap scan report for 10.42.1.179

Host is up (0.59s latency).

Not shown: 996 closed ports

PORT	STATE	SERVICE
81/tcp	open	hosts2-ns
554/tcp	open	rtsp
1935/tcp	open	rtmp
8080/tcp	open	http-proxy

- 81 – Panel WWW
- 554 – RTSP
- 1935 – RTMP
- 8080 – ONVIF

Rekonwersja

IP Camera Options

▶ System Settings

- Device Info

- Time Settings

- System Maintenance

▶ Networking

▶ Advanced Settings

▶ Alarm Settings

▶ Video & Audio Settings

Return

System Maintenance

System Maintenance

Reboot the system:

Restart

Restore factory default values:

Default Values

Backup configuration data:

Save

To restore configuration data:

Wybierz plik

Nie wybrano pliku

OK

System Upgrade:

Wybierz plik

Nie wybrano pliku

OK

Hi3518E V200 Economical HD IP Camera SoC

Processor Core

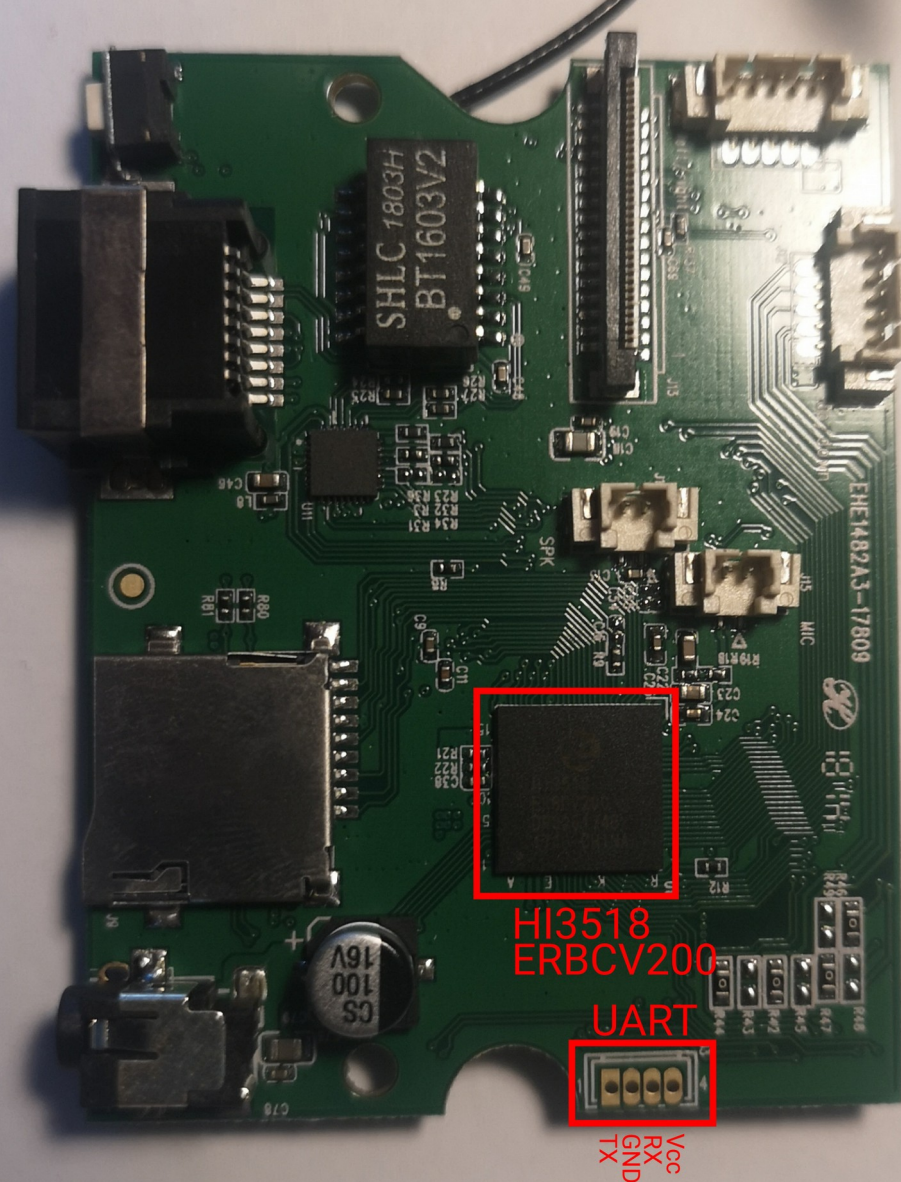
- ARM926@540 MHz, 32 KB I-cache, 32 KB D-cache

SDK

- Linux 3.4-based SDK
- High-performance H.264 PC decoding library

Physical Specifications

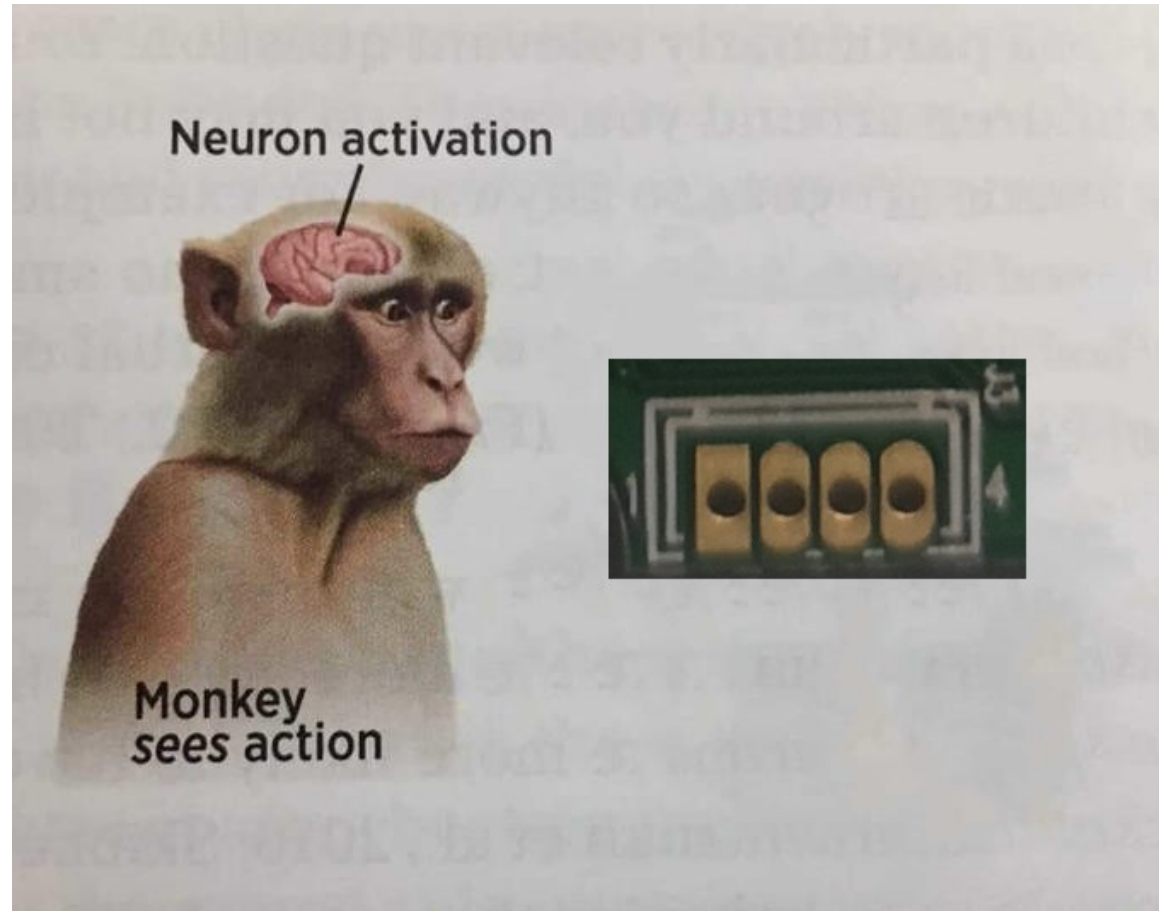
- Operating voltages
 - 1.1 V core voltage
 - 3.3 V I/O voltage and 3.8 V margin voltage



Rekonesans

UART

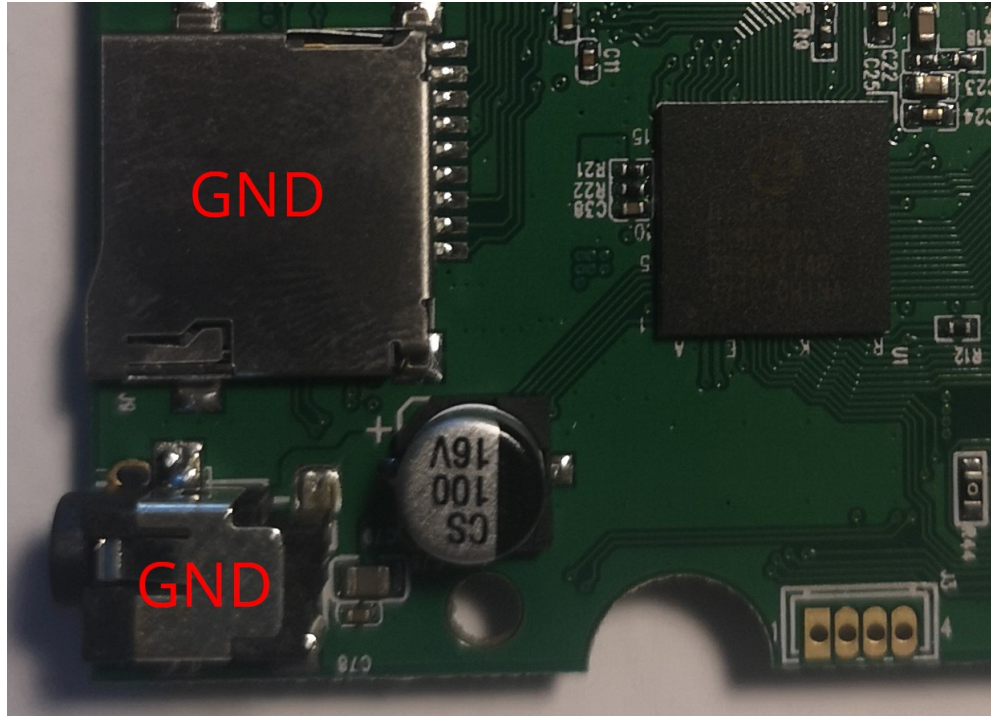
- Prosta transmisja szeregową
- Potrzebne trzy linie: TXD, RXD, GND
- Często używany jako interfejs konsoli
- Może działać już na etapie bootloadera
- Istnieją standardowe prędkości transmisji, ale najczęściej są to: 9600 i 115200 bodów
- Picocom, Putty, RealTerm...



Rekonesans

Ustalanie pinów UART

- GND: Multimetr ustawiamy w tryb testera ciągłości obwodu, jedna końcówka do „masy”, drugą sprawdzamy piny, aż miernik zacznie piszczeć. **Urządzenie musi być wyłączone.**



Rekonesans

Ustalanie pinów UART

- Vcc (jeżeli są cztery piny): Multimetr ustawiamy w tryb woltomierza, jedna końcówka do GND, drugą sprawdzamy piny, aż miernik wyświetli stabilne napięcie zasilania (tutaj 3,3V). **Urządzenie musi być włączone.**
- TXD: Podłączamy interfejs UART-USB. Pin GND interfejsu łączymy z GND urządzenia, RXD interfejsu łączymy z TXD urządzenia. Włączamy urządzenie i obserwujemy transmisję.
- RXD: Ostatni pin, który został po wcześniejszej eliminacji.

Pozyskanie firmware

- Plik z aktualizacją
 - Można spróbować rozpakować narzędziem `binwalk`

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	JFFS2 filesystem, little endian
4456448	0x440000	UBI erase count header, version: 1, EC: 0x0, VID header offset: 0x800, data offset: 0x1000

- Podłuch komunikacji sieciowej podczas wymiany firmware
- Można włamać się do urządzenia i skopiować potrzebne pliki
- Kopiowanie kości flash
 - Wariant tani: <https://www.flashrom.org/> + Raspberry Pi
 - Wariant drogi: dedykowany programator

Uzyskanie dostępu

Przez bootloader (U-boot)

- Sprawdzamy czy konsola bootloadera jest odblokowana.
- Jeżeli jest zablokowana, to można spróbować zakłócić proces ładowania kernela.
- Z poziomu konsoli U-boota można odczytywać i zapisywać dane, zmieniać parametry uruchamiania kernela.
 - `printenv` – polecenie wypisujące wszystkie zmienne środowiskowe bootloadera
 - `bootcmd` – zmienna środowiskowa z komendą/skryptem, wykonywanym automatycznie po uruchomieniu.

Uzyskanie dostępu

Przez błąd w panelu WWW

- Sprawdzamy każde pole przyjmujące dane wejściowe od użytkownika.
- Formularze mogą zawierać błąd „command injection”.
- Warto sprawdzić aplikacje ułatwiające konfigurację urządzenia.
- Ciekawym celem jest funkcja przywracania konfiguracji urządzenia z pliku.

Uzyskanie dostępu

Kopia konfiguracji

- W teorii tajemniczy *.bin, a w praktyce *.tar.gz (`file` i `binwalk` twoimi przyjaciółmi).
- W konfiguracji szukamy opcji deweloperskich oraz miejsc do wstrzyknięcia komendy.
- Czasami `binwalk` jednak zawodzi

Uzyskanie dostępu

Jeden z wpisów w konfiguracji

```
[telnet]
tenable = "0"
```

Skrypty udhcpd: default.bound, default.deconfig, default.leasefail, default.renew, default.script

Skrypty shella uruchamiane po wystąpieniu odpowiedniego zdarzenia związanego z DHCP.

Uzyskanie dostępu

- Po przełączeniu `tenable` został włączony telnet na urządzeniu, ale nadal nie znamy hasła.
- Standardowe wyjście ze skryptów `udhcpd` jest widoczne na porcie szeregowym.
- Ponieważ skrypty są wykonywane z uprawnieniami `roota` to możemy dowolnie odczytywać i modyfikować zawartość `/etc/shadow`.

```
root:$1$tiaLlxGM$byeTUfQgqyET5asfwwNjg0:16199:0:99999:7:::  
admin:$1$rHWQwR5V$i4FVDvwhuzau8msvAfHEt.:16199:0:99999:7:::
```

Uzyskanie dostępu

Kilka sekund później:

```
root:hichiphx  
admin:2601hx
```

Właśnie uzyskaliśmy dostęp do powłoki systemowej.

Na co patrzeć

- Uprawnienia procesów.
- Ochrona przed eksploatacją (checksec).

RELRO	STACK CANARY	NX	PIE	RPATH	RUNPATH	Symbols	FORTIFY	Fortified	Fortifiable	FILE
No RELRO	No canary found	NX disabled	No PIE	No RPATH	No RUNPATH	No Symbols	No	0	17	ipc_server

- Wersje aplikacji i bibliotek - Software Bill of Materials (SBOM).
 - Lista już istniejących CVE.
 - Warto zapytać o backporty.
 - **Aplikacje producenta.**
- Sposób komunikacji urządzenia z innymi systemami (protokoły, szyfrowanie itp).
- **Backdoory** Nieudokumentowane funkcje administracyjne.



gwire

@gwire@mastodon.social

Closed source software doesn't have backdoors.

It does have "undocumented administrative features" and "development tools mistakenly enabled in production", but not backdoors.

Mar 30, 2024, 12:06 PM · 🌐 · Ivory for iOS

Na co patrzeć

- Wstrzyknięcia danych.
- Weryfikacja podpisu firmware.
- Czy firmware jest modyfikowalny?
- Ochrona wrażliwych danych (hasła, klucze, tokeny itp.).
- W jaki sposób urządzenie omija NAT?
- W jaki sposób nowe urządzenie jest parowane z kontem użytkownika w chmurze?

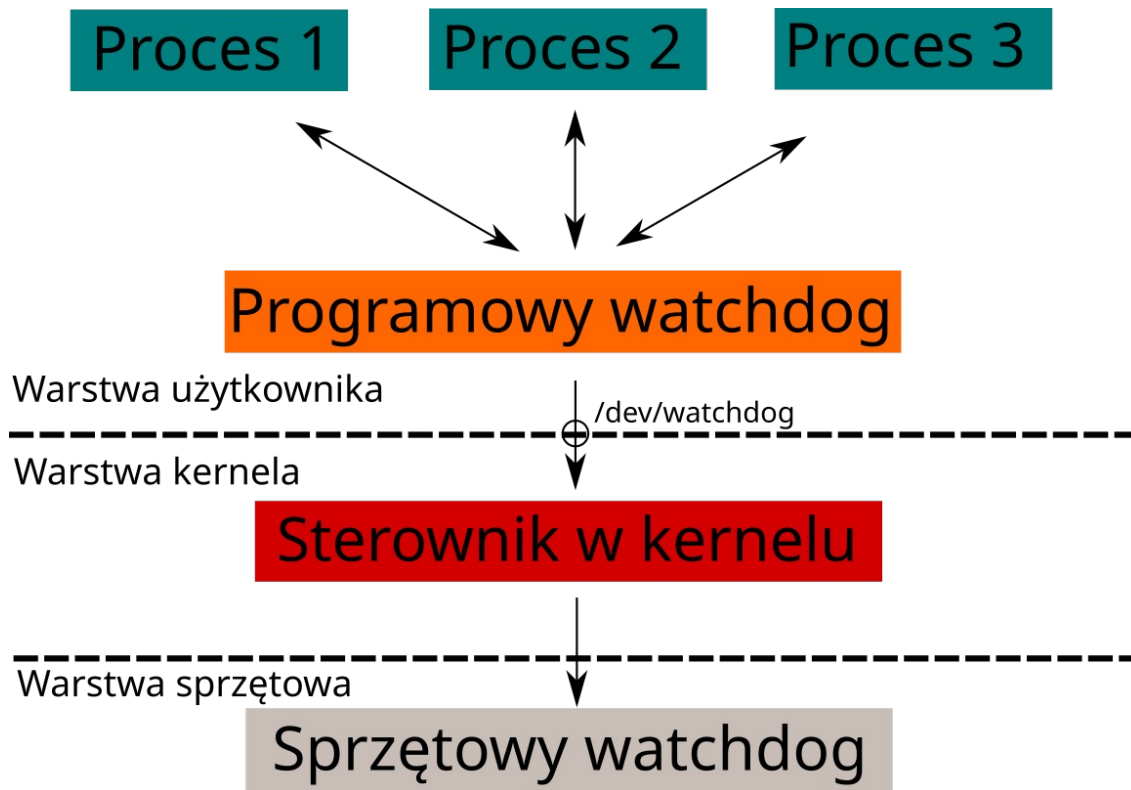
Na co patrzeć

- **netstat -atulpn**

Active Internet connections (servers and established)

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	0.0.0.0:554	0.0.0.0:*	LISTEN	954/ipc_server
tcp	0	0	0.0.0.0:1935	0.0.0.0:*	LISTEN	954/ipc_server
tcp	0	0	0.0.0.0:8080	0.0.0.0:*	LISTEN	1075/onvif
tcp	0	0	0.0.0.0:81	0.0.0.0:*	LISTEN	954/ipc_server
tcp	0	0	0.0.0.0:23	0.0.0.0:*	LISTEN	860/telnetd
tcp	0	0	127.0.0.1:81	127.0.0.1:42504	ESTABLISHED	954/ipc_server
tcp	0	0	10.42.1.179:23	10.42.1.1:33202	ESTABLISHED	860/telnetd
tcp	0	0	127.0.0.1:42609	127.0.0.1:81	ESTABLISHED	1415/tutk
tcp	0	0	127.0.0.1:81	127.0.0.1:42609	ESTABLISHED	954/ipc_server
tcp	0	0	127.0.0.1:42504	127.0.0.1:81	ESTABLISHED	1075/onvif
udp	0	0	0.0.0.0:8002	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:12109	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:12129	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:3702	0.0.0.0:*		1048/onvif
udp	0	0	0.0.0.0:12222	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:6600	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:6601	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:6602	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:6603	0.0.0.0:*		954/ipc_server
udp	0	0	0.0.0.0:47564	0.0.0.0:*		1415/tutk
udp	0	0	0.0.0.0:32761	0.0.0.0:*		1415/tutk

- Warto wyłączyć watchdoga



Badamy backdoory

- Zaczynamy mozolną analizę...
- Jeden z backdoorów był już wcześniej znany – wykrywanie kamery w sieci lokalnej, odczyt Device-ID, reset hasła administratora bez uwierzytelniania, włączenie telnetu (CVE-2020-9529, <https://github.com/tothi/malicious-hisilicon-scripts>)
- Nieopisana wcześniej usługa na porcie 12129.

Badamy backdoory

- Podsumowanie analizy nowego backdoora
 - Usługa czeka na dane multicastowe wysłane na adres 239.255.255.252, port 12129 UDP.
 - Budowa ramki:
 - stała wartość 0xf9f9f9f9,
 - 3 bajty z losowymi wartościami,
 - pierwsze osiem bajtów wartości Device-ID
 - 1-bajtowa suma kontrolna pierwszej połowy Device-ID (XOR),
 - ostatnie osiem bajtów wartości Device-ID,
 - 1-bajtowa suma kontrolna drugiej połowy Device-ID,
 - 7 bajtów z losowymi wartościami.
 - Ukryta funkcja aktywowana po wysłaniu ramki z pierwszą połówką Device-ID inną niż na urządzeniu.

Badamy backdoory

- Po aktywowaniu program usunie trzy pliki:
 - `/mnt/mtd/ipc/modules/hi3518e_base.ko`
 - `/mnt/mtd/ipc/conf/config_encode.ini`
 - `/mnt/mtd/ipc/chksensor`
- Robimy kopię zapasową tych plików, odpalamy exploit...
- ... i uceglamy urządzenie
- Urządzenie niby działa, ale nie do końca ;_;
- Błąd typu DoS

Badanie komunikacji

- W zaproponowanym środowisku testowym można obserwować całą komunikację sieciową urządzenia.
- Komunikacja HTTP → proxy OWASP ZAP.
 - W przypadku aplikacji na smartfony trzeba zainstalować certyfikat CA serwera proxy.
- Inne protokoły → Wireshark i inne narzędzia.
- W przypadku badanej kamery:
 - Komunikacja między aplikacją na Androida i chmurą producenta bazowała na HTTPS.
 - Komunikacja między aplikacją na Androida i kamerą była realizowana przy pomocy autorskiego protokołu P2P firmy ThroughTek.
 - Oczywiście „własna kryptografia” jest łatwa do odszyfrowania (wkompilowany na stałe klucz „Charlie is the designer of P2P!!”).

Kontakt z producentem

- Sytuacja idealna:
 - Producent ma dedykowany sposób kontaktu do zgłaszania błędów bezpieczeństwa.
 - Po otrzymaniu zgłoszenia producent ponawia analizę po swojej stronie.
 - Wychodzi nowy firmware z naprawionymi błędami.
 - Producent współpracuje przy rejestrowaniu nowego CVE i publikowaniu informacji.
 - Sława i chwała za zgłoszenie błędu...

Kontakt z producentem

- Brutalna rzeczywistość:
 - „Producent” kamery posiada tylko jedną wersję firmware – tą, z którą jest sprzedawane urządzenie.
 - Brak chęci/deklaracji w kwestii wydania poprawionego firmware.
 - „Proszę oczywiście o nieupublicznianie swoich testów w kontekście konkretnego typu kamery.”
 - To może chociaż prawdziwy autor oprogramowania będzie zainteresowany...

Kontakt z producentem

- Shenzhen Hichip Vision Technology
 - Brak dedykowanego maila
 - Kilka prób kontaktu na ogólny adres pozostało bez odpowiedzi
 - Nie da rady drzwiami, to spróbujmy oknem...

Kontakt z producentem

- Paul Marrapese (<https://hacked.camera/>) zgłosił kilka błędów powiązanych z produktami Shenzhen Hichip Vision Technology.
 - DEF CON 28 - Abusing P2P to Hack 3 Million Cameras
- Paul umożliwił mi kontakt z jednym z pracowników..

Kontakt z producentem

Oficjalne stanowisko firmy:

A specially crafted multicast message only can deactivate a given copyrighted camera and its clone ones, but it can't deactivate other copyrighted cameras. We used this intellectual property protection feature only in some special kind of cameras in 2017 for a very short time, it only affects about several thousand 'clone' cameras. When we realized that it maybe hurt not only the illegal factory but also the innocent end users, we removed it soon.

Zgłaszamy nowe CVE

- CVE Numbering Authority (CNA).
- <https://www.cve.org/PartnerInformation/ListofPartners>
- Najpierw szukamy dedykowanego CNA.
- Jeżeli nie ma dedykowanego CNA, to zgłaszamy błąd do jakiegoś „ogólnego” CNA.
- Warto podesłać swoją propozycję CVSS.

Partner	Scope	Program Role	Organization Type	Country*
Android (associated with Google Inc. or Open Handset Alliance)	Android issues, as well as vulnerabilities in third-party software discovered by Android that are not in another CNA's scope	CNA	Vendor, Open Source, Researcher	USA

Zgłaszamy nowe CVE

Partner	Scope	Program Role	Organization Type	Country*
Debian GNU/Linux	Debian issues only	CNA	Vendor, Open Source	USA
GNU C Library	Security issues and vulnerabilities in the GNU C Library	CNA	Open Source	USA

Partner	Scope	Program Role	Organization Type	Country*
Siemens	Siemens issues only	CNA	Vendor	Germany

Partner	Scope	Program Role	Organization Type	Country*
Moxa Inc.	Moxa products only	CNA	Vendor	Taiwan





Zgłaszamy nowe CVE

Partner	Scope	Program Role	Organization Type	Country*
CERT.PL	Vulnerabilities in software discovered by CERT.PL, and vulnerabilities reported to CERT.PL for coordinated disclosure, which are not in another CNA's scope	CNA	CERT	Poland








Zgłaszamy nowe CVE

- <https://incydent.cert.pl/>

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

 Osoba fizyczna / inne podmioty	 Operator usług kluczowych	 Dostawca usługi cyfrowej	 Podmiot publiczny
---	--	---	--

Prosimy o wybranie odpowiedniej kategorii:

 Złośliwa domena Domeny wyludzające dane osobowe lub środki finansowe	 Podejrzana wiadomość SMS Treść wiadomości SMS	 Podejrzana wiadomość e-mail Podejrzane załączniki, phishing, szantaż	 Oszustwo Fałszywe sklepy internetowe i inne próby podszywania się
 Złośliwe oprogramowanie Próbki wirusów lub pliki zaszyfrowane ransomware	 Podatności Błędy w oprogramowaniu lub aplikacjach internetowych	 Nielegalne treści Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl	Inne Wszystkie inne incydenty niepasujące do poprzednich kategorii

Zgłaszamy nowe CVE

nvd.nist.gov/vuln/detail/CVE-2022-23382

CVE-2022-23382 Detail

Description

Shenzhen Hichip Vision Technology IP Camera Firmware V11.4.8.1.1-20170926 has a denial of service vulnerability through sending a crafted multicast message in a local network.

Severity

CVSS Version 3.x

CVSS Version 2.0

CVSS 3.x Severity and Metrics:



CNA: MITRE

Base Score: **8.1 HIGH**

Vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

Pytania?