(In)Sicurezza Informatica dei dispositivi

Dalle IP camere alle automobili connesse

Dario Stabili
Ricercatore
Alma Mater Studiorum - Università di Bologna

dario.stabili@unibo.it

Linux Day 2023 - FUM - 28 ottobre 2023

A.C.E.S

Domanda semplice: cosa fa questo codice?

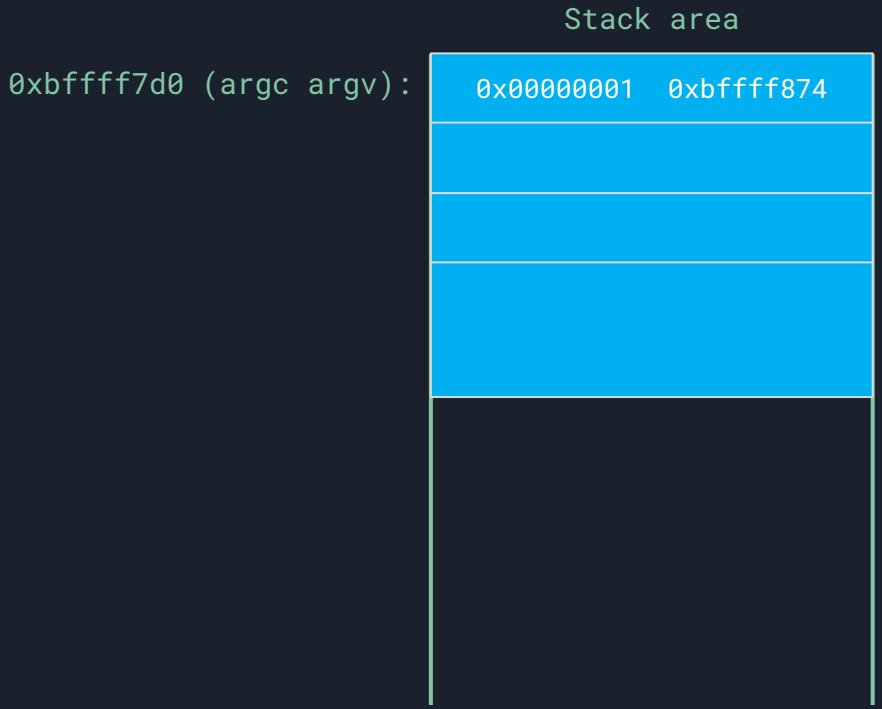
```
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```

Domanda semplice: cosa fa questo codice?
Espone una vulnerabilità

```c
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```

Domanda semplice: cosa fa questo codice?
Espone una vulnerabilità

```c
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```

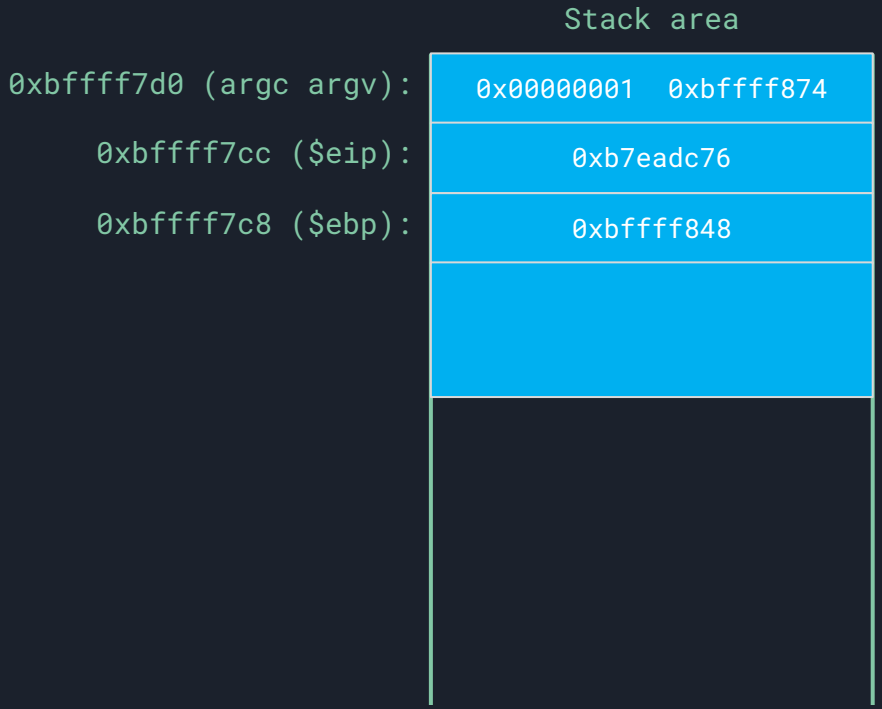


Domanda semplice: cosa fa questo codice?
Espone una vulnerabilità

```c
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```

Domanda semplice: cosa fa questo codice?
Espone una vulnerabilità

```c
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```

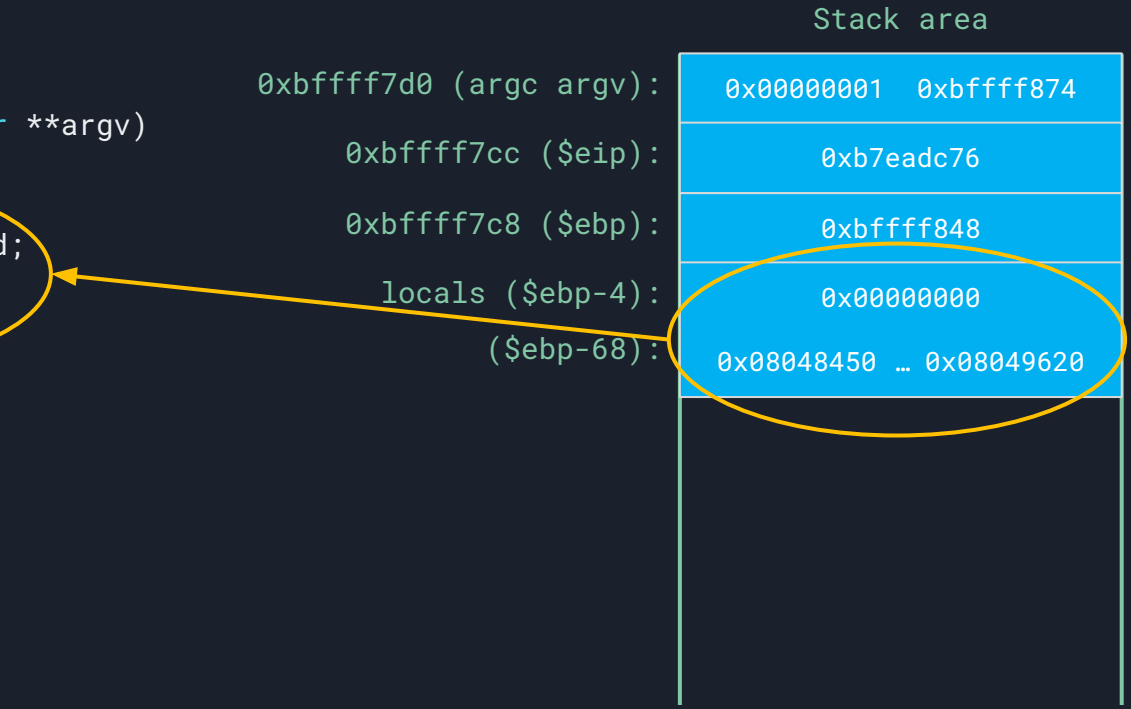


Domanda semplice: cosa fa questo codice?
Espone una vulnerabilità

```c
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```

Domanda semplice: cosa fa questo codice?
Espone una vulnerabilità

```
int main(int argc, char **argv)
{
  volatile int modified;
  char buffer[64];

  modified = 0;
  gets(buffer);
}
```



Caso studio: IP Camera Tenda CP3

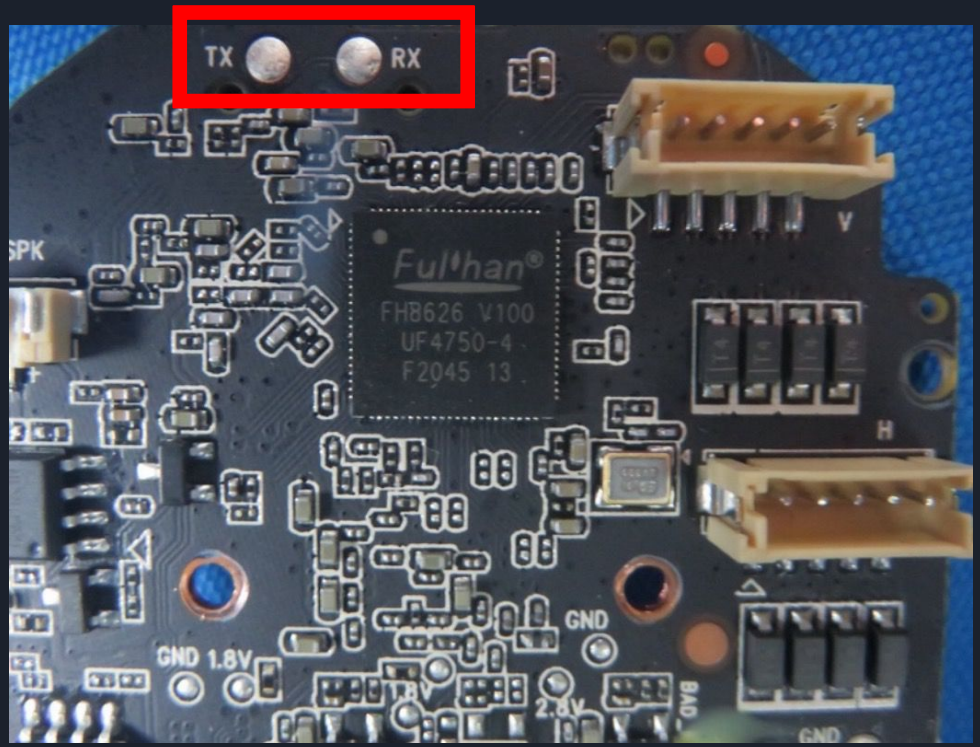
Caso studio: IP Camera Tenda CP3

Analisi di sicurezza della telecamera

1. [HW] Trovare interfacce sulla videocamera
2. [HW] Ottenere quante più informazioni dalla camera
3. [HW] (Se possibile) acquisire firmware
4. [SW] Analizzare servizi aperti
5. [SW] Definire exploit
6. [SW] Elevazione di privilegi

A.C.E.S

Caso Studio: IP Camera Tenda CP3



Caso Studio: IP Camera Tenda CP3

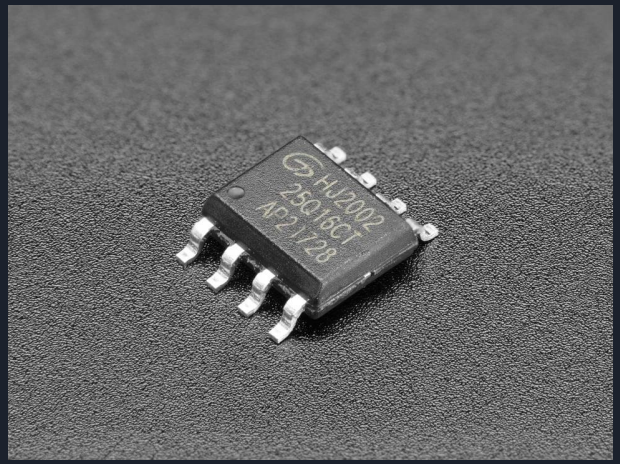
minicom bootlog

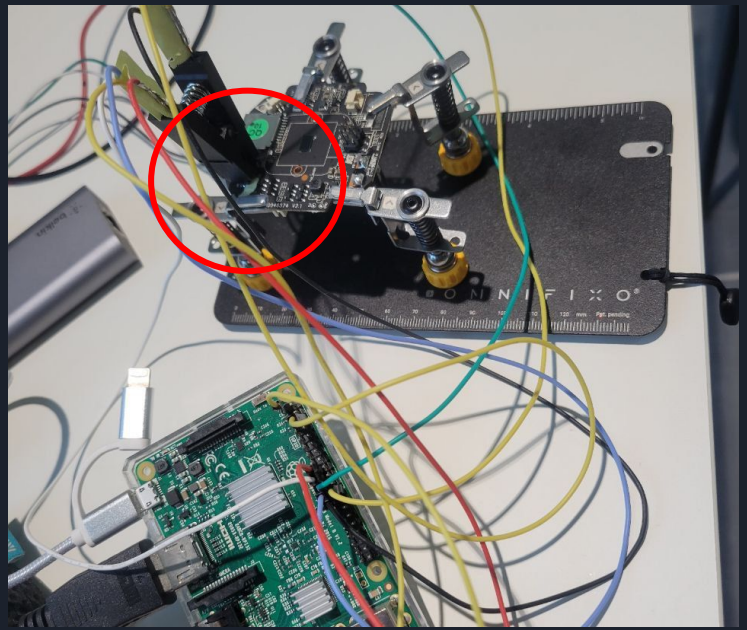
```
ROM:    Use nor flash.

U-Boot 2010.06-dirty (Sep 07 2021 - 16:46:09)
DRAM:  64 MiB
Press 'E' to stop autoboot
verify flash image OK

load kernel 0x00050000(0x002e0000) to 0xa1000000
## Booting kernel from Legacy Image at a1000000 ...
   Image Name:   Linux-3.0.8
   Created:      2021-09-07   8:49:48 UTC
   Image Type:   ARM Linux Kernel Image (uncompressed)
OK
```

minicom bootlog

```
6 cmdlinepart partitions found on MTD device spi_flash
Creating 6 MTD partitions on "spi_flash":
0x000000000000-0x000000010000 : "bootstrap"
0x000000010000-0x000000020000 : "uboot-env"
0x000000020000-0x000000050000 : "uboot"
0x000000050000-0x000000350000 : "kernel"
0x000000350000-0x0000003d0000 : "data"
0x0000003d0000-0x000000800000 : "app"

Please press Enter to activate this console.
(none) login:
```

Caso Studio: IP Camera Tenda CP3





Caso Studio: IP Camera Tenda CP3

super_secure_script.sh

```
if [ -d /mnt/sd/upgrade ] ; then
    if [ -f /mnt/sd/upgrade/img_up ] ; then
        cp /mnt/sd/upgrade/img_up /home/
        chmod +x /home/img_up
    fi
    if [ -f /mnt/sd/upgrade/iu.sh ] ; then
        cp /mnt/sd/upgrade/iu.sh /home/
    elif [ -f /usr/bin/iu.sh ] ; then
        cp /usr/bin/iu.sh /home/
    elif [ -f $cur_dir/iu.sh ] ; then
        cp $cur_dir/iu.sh /home/
    fi
    if [ -f /home/iu.sh ] ; then
        chmod +x /home/iu.sh
        /home/iu.sh -s
    fi
    rm -f /home/iu.sh
        rm -f /home/iu_s.sh
```

A.C.E.S

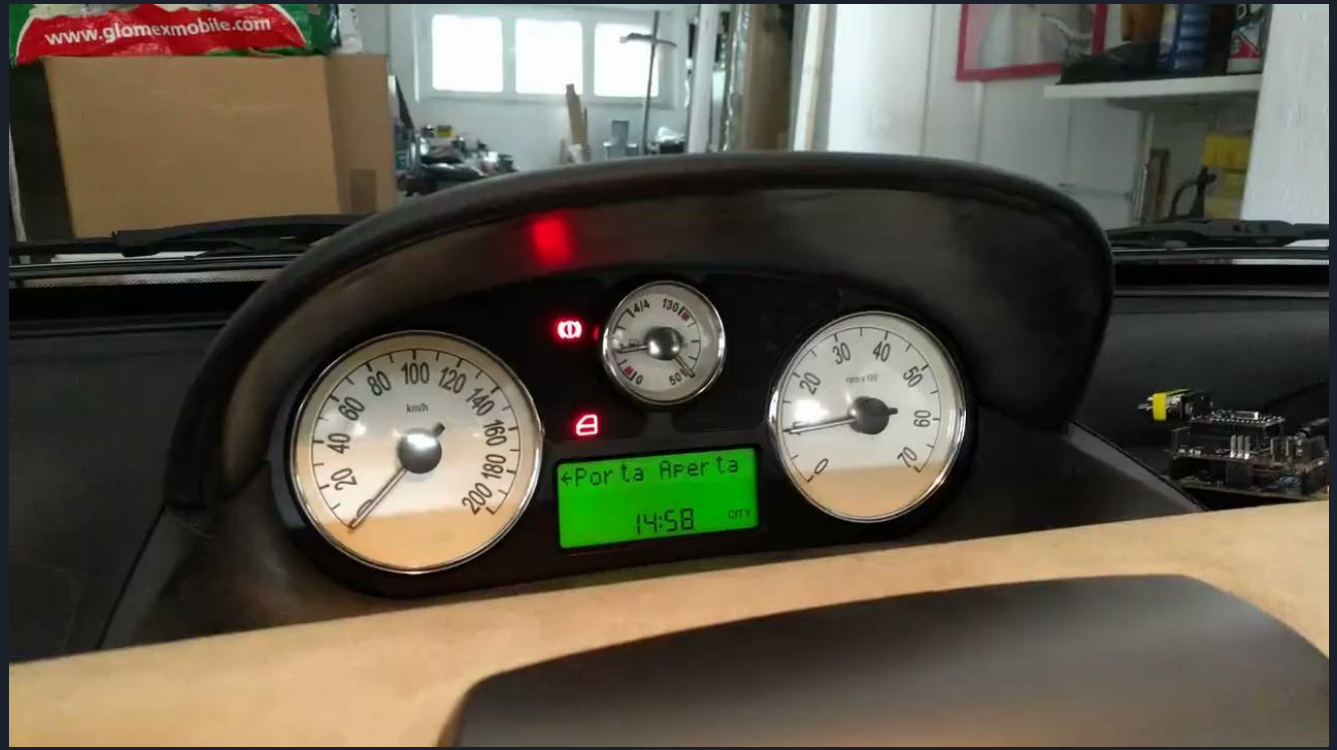
Caso Studio: IP Camera Tenda CP3

CVE ID	Nome	CVSS
CVE-2023-30351	Remote access via hard-coded credentials	7.5 HIGH
CVE-2023-30352	RTSP feed access via hard-coded credentials	9.8 CRITICAL
CVE-2023-30353	Unauthenticated RCE	9.8 CRITICAL
CVE-2023-30354	Physical access and WiFi credentials disclosure	9.8 CRITICAL
CVE-2023-30356	Missing support for Integrity Check	7.5 HIGH

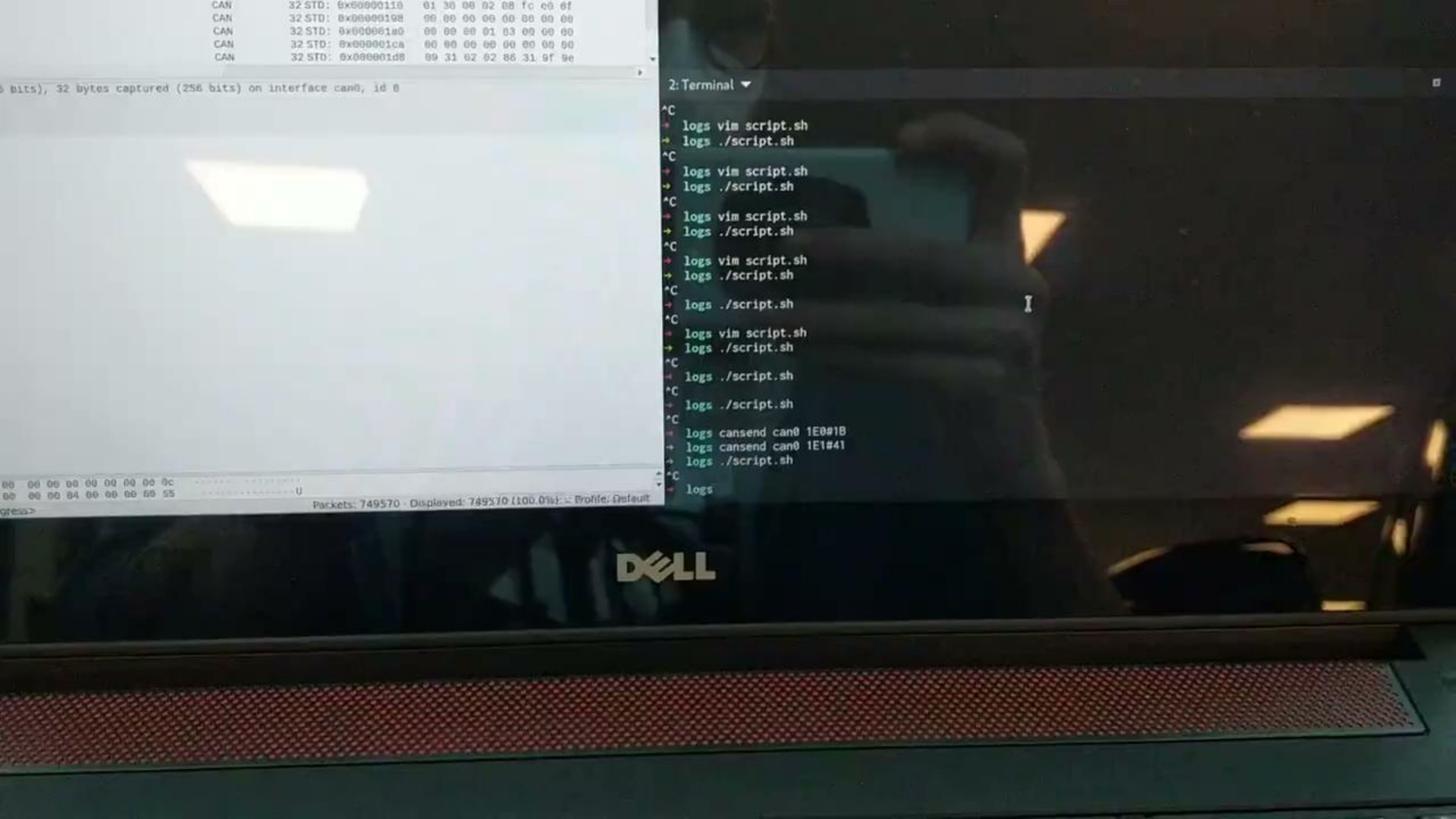
https://github.com/SECloudUNIMORE/ACES/tree/master/Tenda

Case Study: Automotive

(very old) PoC: Denial of Service



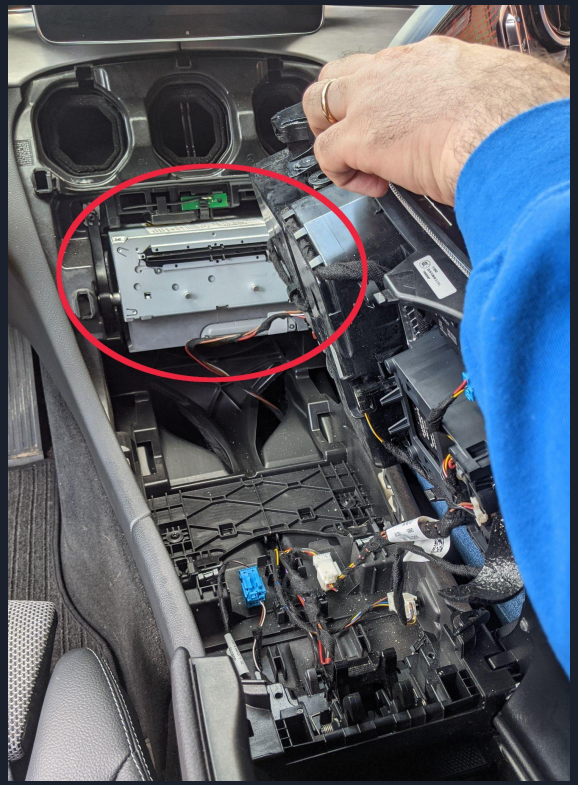
(very old) PoC: ECU Spoofing


CAN 32 STD: 0x00000110 01 30 00 02 08 fc e0 6f
CAN 32 STD: 0x00000198 00 00 00 00 00 00 00 00
CAN 32 STD: 0x000001a0 00 00 00 01 03 00 00 00
CAN 32 STD: 0x000001ca 00 00 00 00 00 00 00 00
CAN 32 STD: 0x000001d8 09 31 02 02 86 31 9f 9e
bits), 32 bytes captured (256 bits) on interface can0, id 0
Packets: 749570 · Displayed: 749570 (100.0%) · Profile: Default
2: Terminal
^C
logs vim script.sh
logs ./script.sh
logs cansend can0 1E0#1B
logs cansend can0 1E1#41
logs


VOLVO
FF 897NB


DELL

Privacy nei sistemi automotive



Privacy nei sistemi automotive