

Hacking de capteur de glycémie connecté

Axelle Apvrille (Fortinet)
Travis Goodspeed

*Unlock Your Brain
Harden Your System
UYBHYS*

Novembre 2020

FORTINET®

Bonjour !



Axelle Apvrille

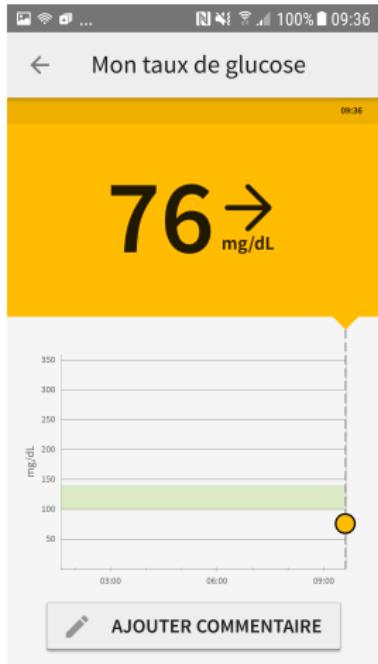
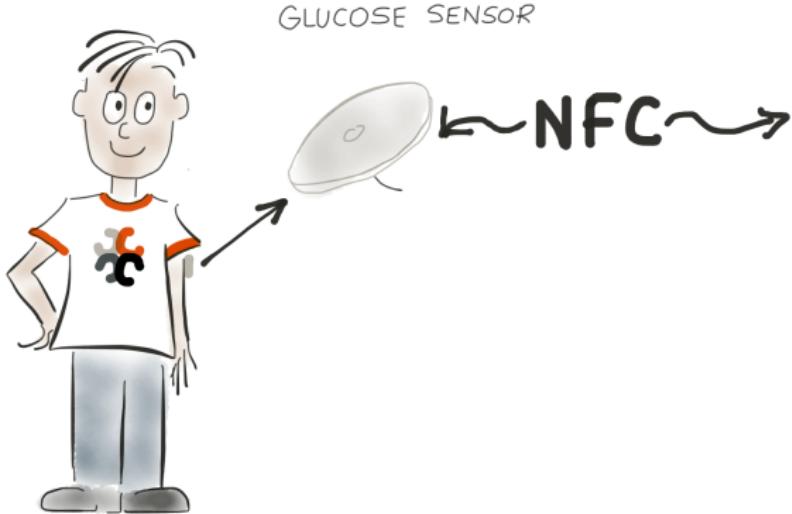
Principal Security Researcher chez
Fortinet, @cryptax
Mobile malware, IoT, Ph0wn CTF



Travis Goodspeed

Digital watchmaker and Studebaker
enthusiast, @travisgoodspeed
GoodFET, GoodWatch, PoC||GTFO

FreeStyle Libre: c'est vraiment utile !



Evite de devoir se piquer trop souvent

Cycle de vie d'un capteur

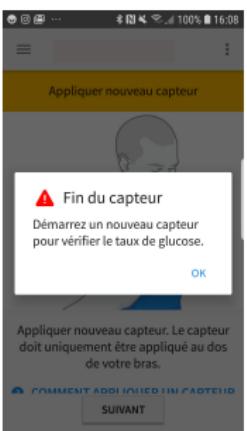
Monter le capteur



Appliquer le capteur



Délai d'activation (60 min) On peut l'utiliser !



Expiration (14 j)

Hacking



- ① Réinitialisation du capteur
- ② Durée d'activation
- ③ Zonage du capteur
- ④ Longévité du capteur
- ⑤ Modifier les valeurs de glycémie

Ces hacks fonctionnent sur le
FreeStyle Libre, mais n'ont pas été
testés sur le tout **nouveau**
FreeStyle Libre 2*

* Disponibles en France seulement depuis
Juin 2020, vendus en ligne, pas encore
remboursés par la Sécu.

Avertissement d'usage !



Ces hacks fonctionnent d'un point de vue
technique

Ils n'ont pas été testés d'un point de vue médical et peuvent être dangereux. Nous vous **déconseillons de “jouer” avec.**

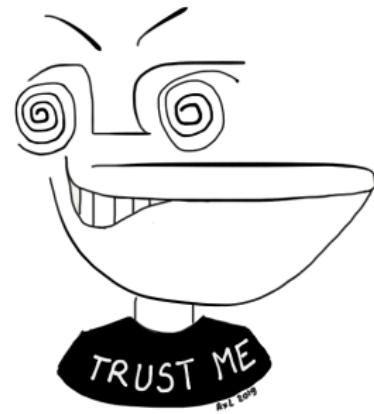
mais un attaquant pourrait le faire...

Démo: résurrection

Principe

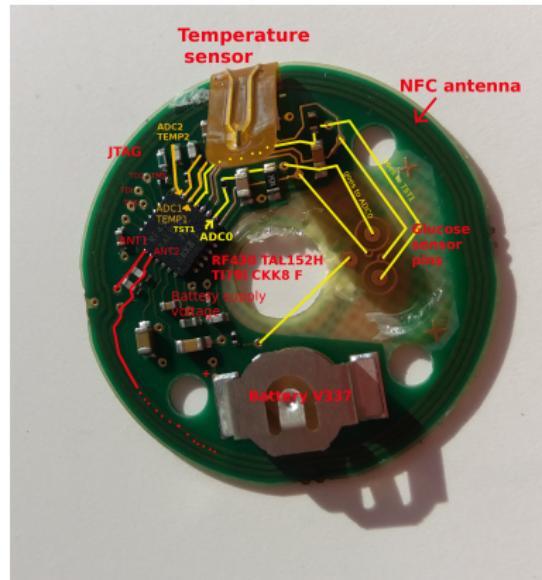
- Le capteur a expiré
- Magie* ! On le ramène à la vie !
- Il faut l'activer (comme un capteur neuf)
- Attendre le délai d'activation (comme un capteur neuf)
- Puis l'utiliser ! (eh, attention, il n'est pas vraiment neuf !)

* En fait, non, il n'y a rien de magique



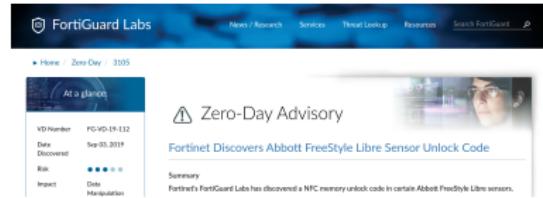
Les étapes de notre démarche

- ① Démontage de l'objet: il y a une puce
TI RF 430 TAL



Les étapes de notre démarche

- ① Démontage de l'objet: il y a une puce
TI RF 430 TAL
- ② Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)



The screenshot shows a web interface for FortiGuard Labs. At the top, there's a navigation bar with links for Home, News / Research, Services, Threat Lookup, Resources, and a search bar. Below the header, a banner features a person wearing a headset and the text "At a glance". The main content area displays a "Zero-Day Advisory" card. The card has a blue header with the text "At a glance" and a warning icon. Below the header, there's a summary section with the text "Fortinet Discovers Abbott FreeStyle Libre Sensor Unlock Code". The advisory card contains the following details:

- VD Number: PG-VD-19-132
- Date Discovered: Sep 03, 2019
- Risk: ● ● ●
- Impact: Data Manipulation

Les étapes de notre démarche

- ① Démontage de l'objet: il y a une puce
TI RF 430 TAL
- ② Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)
- ③ Dump du firmware, via NFC



Les étapes de notre démarche

- ① Démontage de l'objet: il y a une puce **TI RF 430 TAL**
 - ② Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)
 - ③ Dump du firmware, via NFC
 - ④ Reverse du firmware, identification d'une fonction désactivée (E0) pour le reset

```

***** FUNCTION *****

undefined run_calledby_e0()
R12_1:l1    .RETURN
R15:2      addr
R14_1:l1    len
XREF[1]: 52
XREF[2]: 52
XREF[3]: 52
XREF[4]: 1c72(*), 52
PUN_514*: 52
fram_e0:fbc

5256 0a 12    PUSH.W   R10
5256 b2 40 80  MOV.W    #0x5aB2,B#NOTCTL
5a 5c 01
5256 54 42 03 08 MOV.B    #0#F13MINT_H,R10
5262 c2 43 03 08 MOV.B    #0,#F13MINT_H
5266 3f 40 7a f8 MOV.W    #0xb187a,addr
526a 7e 40 93 00 MOV.B    #0#93,R14

zeroize trend record table and history table: we zeroize 0x93...
LAB_526e
526e 8f 43 00 00 MOV.W    #0,0x(addr)==>trend_index
XREF[1]: 5276(j)
5272 2f 53     INCD.W   addr
5274 7e 53     ADD.B    #-1,len
5276 fb 23     JNE      LAB_526e
5278 e2 12 c3 1c BIT.B    #4,#DAT1_cc3
5276 16 28     JNC      LAB_52aa
5276 3f 40 66 f8 MOV.W    #0#f666,addr
5262 7e 40 09 00 MOV.B    #0#93,len

zeroize 0x80 words after the expiration indicator in the head...
LAB_5286
5286 8f 43 00 00 MOV.W    #0,0x(addr)==>DAT_F866
XREF[1]: 528e(j)
528a 2f 53     INCD.W   addr
528e 7e 53     ADD.B    #-1,len
5286 fb 23     JNE      LAB_5286
5290 c2 43 65 f8 MOV.B    #0,#fram_expirationindicator
5294 0f 43      MOV.W    #0,addr-
Start a

```

Les étapes de notre démarche

- ① Démontage de l'objet: il y a une puce
TI RF 430 TAL
- ② Petit à petit, identification d'une commande NFC, **A3**: lecture de n'importe quelle adresse (mot de passe nécessaire)
- ③ Dump du firmware, via NFC
- ④ Reverse du firmware, identification d'une fonction désactivée (E0) pour le reset
- ⑤ Implémentation d'une appli Android



The screenshot shows a mobile application interface with the title "GoodV". The device information is as follows:

INFO:	0004ae10cf0300a007e0f307
SERIAL:	e007a00003cf10ae
VARIANT:	GCM
BLOCKLEN:	8
PAGE:	0
JTAGLOCK:	UNLOCKED
RESET VEC:	da50
STAGE:	Expired
INDICATOR:	00
STATE:	00df0000010000
WEAR :	21530 minutes
REGION:	France
Trend idx:	9
Hist idx:	11

At the bottom right of the app screen is a red circular button with a white envelope icon and the text "EXPORT TO CLIPBOARD".

Sections du capteur et CRC

Section	Début	Fin
Blocs d'activation	F860	F877
Mesures de glycémie	F878	F99F
Capteur et région	F9A0	F9B7
Commandes	F9B8	FFCF
Suffixe	FFD0	FFF7

Adresses des sections applicatives sur le capteur

Infos complètes: rapport technique
(38 pages)

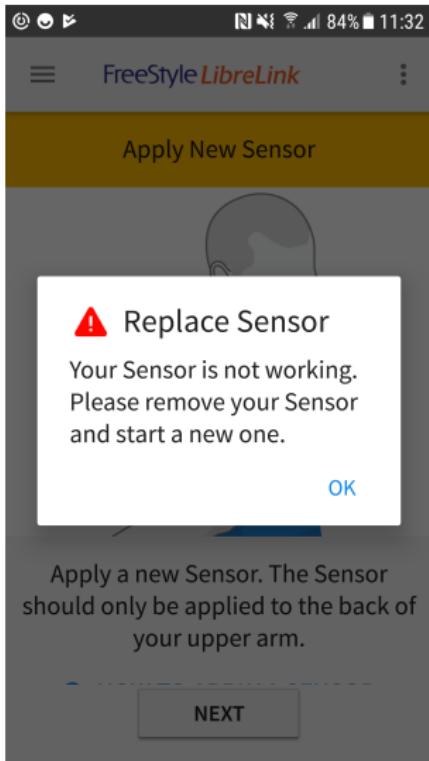


Exemple : section des mesures

Assassinat d'un capteur

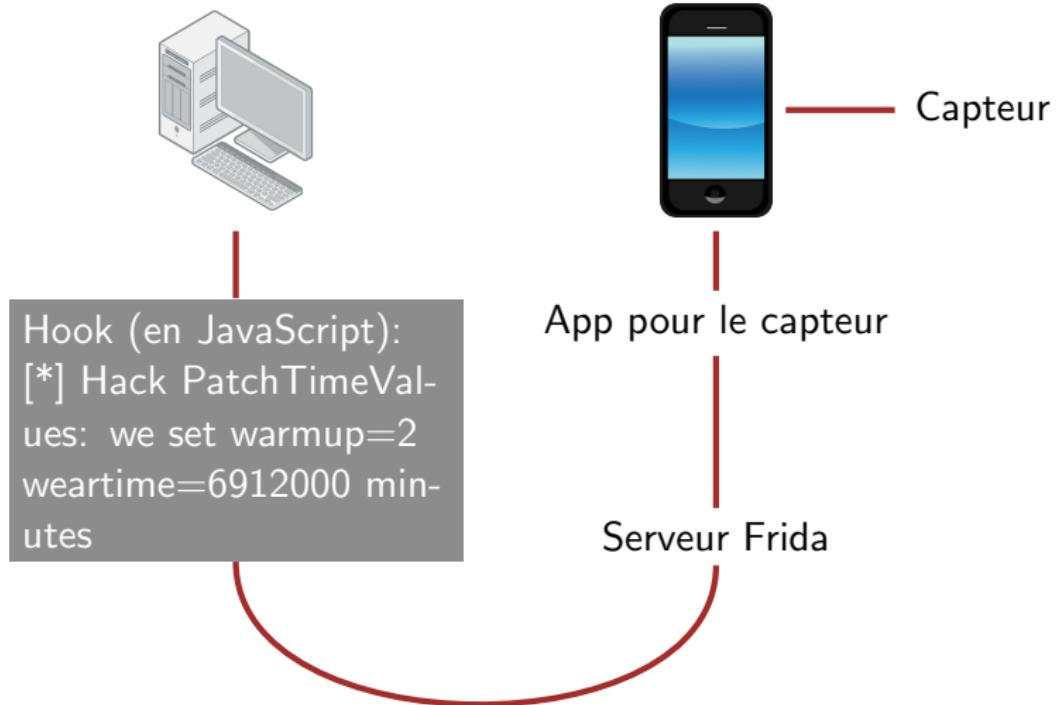
Deux façons de faire:

- Sale: corruption de la mémoire.
- Propre: modifier l'état du capteur vers "expiré".



Exemple : corruption mémoire

Démo: hack de l'activation avec Frida



Récapitulatif des hacks

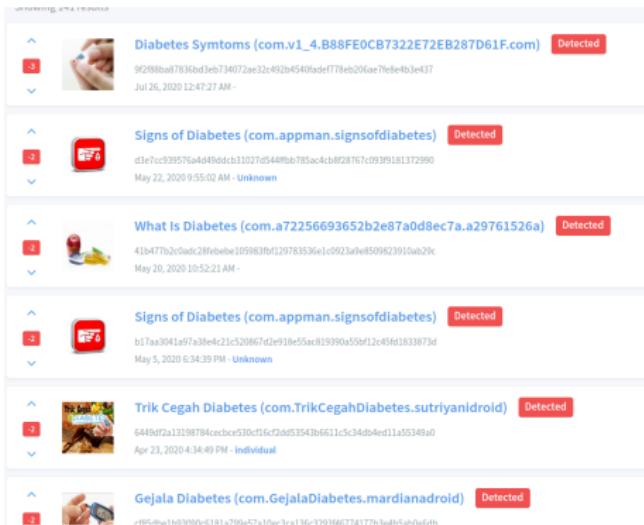
Hack	Conditions	Mise en place
Réssusciter	Proximité + secret	Facile
Assassinat	Proximité + secret	Très facile
Durée d'activation	Lab	Difficile
Longévité	Lab	Difficile
Niveau de glycémie	Lab	Difficile
Zone	Proximité + secret	Facile

Vulnérabilités remontées au fabricant,
a priori ne sont plus présentes dans Libre 2.

Que ferait un attaquant ?

C'est bien plus facile
d'infecter le téléphone avec
un **rançongiciel** !

Les malwares “pour
diabétiques”, ça existe !



The screenshot shows a search results page for "Diabetes" on a mobile device. There are six results listed:

- Diabetes Symtoms (com.v1_4.B88FE0CB7322E72EB287D61F.com)** [Detected] - Jul 26, 2020 12:47:27 AM - A hand holding a syringe icon.
- Signs of Diabetes (com.appman.signsofdiabetes)** [Detected] - May 22, 2020 9:55:02 AM - Unknown - A red smartphone icon.
- What Is Diabetes (com.a72256693652b2e87a0d8ec7a.a29761526a)** [Detected] - May 20, 2020 10:52:21 AM - A small icon of a person's arm with a blood drop.
- Signs of Diabetes (com.appman.signsofdiabetes)** [Detected] - May 5, 2020 6:34:39 PM - Unknown - A red smartphone icon.
- Trik Cegah Diabetes (com.TrikCegahDiabetes.sutriyanidroid)** [Detected] - Apr 23, 2020 4:34:49 PM - Individual - An icon featuring a person and a blood glucose meter.
- Gejala Diabetes (com.GejalaDiabetes.mardianandroid)** [Detected] - A small icon of a hand holding a syringe.

Et FreeStyle Libre 2 ?

La FRAM est chiffrée par un algorithme propriétaire:

- Génération d'une clé de bloc basée sur l'id du capteur, le modèle, magic, et le numéro du bloc
- XOR avec la clé

```
axelle@boostix ~/git/IoT/diabete/prog $ python3 readlibre2.py
Reading .../memory-dumps/libre2-E007A400011DDAC4.dump -----
Status indicator      : Expired
Expiration indicator: Inactive
Trend index          : 9
Historic index       : 9
Trend Glucose level : 1.7 mg/dL
Historic Glucose lev: 220.7 mg/dL
Wear time             : 21498 minutes (i.e 14 days, 22:18:00 hours)
Sensor region         : Europe / UK
Header CRC            : read=c121 computed=c121 OK
Record CRC            : read=d0f0 computed=d0f0 OK
```

Demo

Références

- Rapport complet sur le capteur de glycémie
- GoodV Android application
- Outil pour la lecture du FreeStyle Libre
- NFC exploitation with RF430RFL152 and 'TAL152, PoC || GTFO, 20:03

Merci pour votre attention

Nous contacter :
@cryptax @travisgoodspeed

Merci particulièrement à

- Contacts diabétiques (je garde anonyme!)
- Et: @aamirlakhani @PagetPhil @TuxDePoinsisse @aurelsec
@UYBHYS

Je serais bien venue déguster des galettes bretonnes... snif