

# 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**



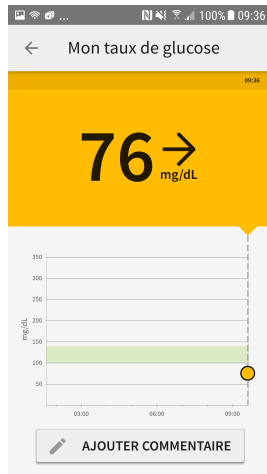
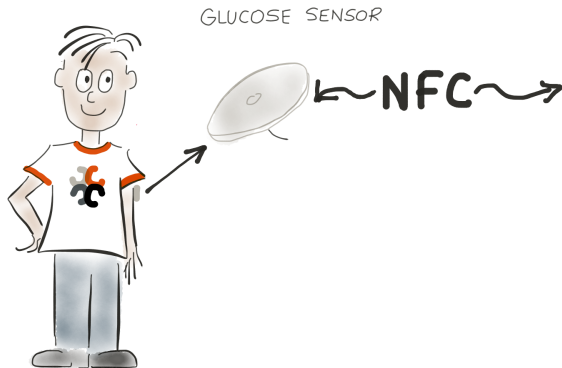
**Travis Goodspeed**

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

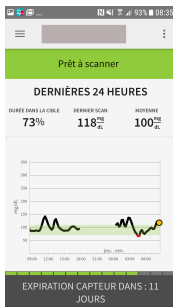
Monter le capteur



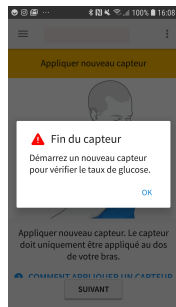
Appliquer le capteur



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.**

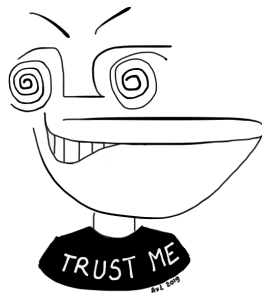
mais un attaquant pourrait le faire...

# Démo: résurrection

## Principe

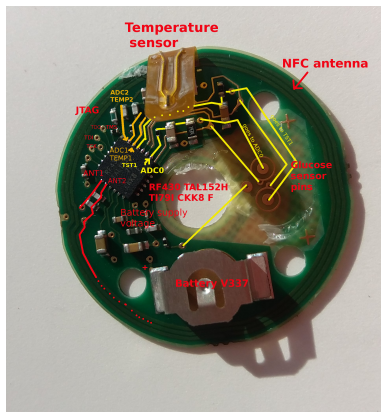
- Le capteur a expiré
- Magie\* ! On le ramène à la vie !
- Il faut l'activer (comme un capteur neuf)
- Attendre le délai d'activation (comme un capteur neuf)
- Puis l'utiliser ! (euh, attention, il n'est pas vraiment neuf !)

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



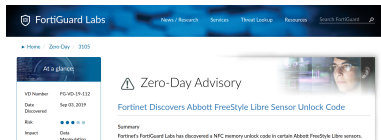
# Les étapes de notre démarche

- 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)



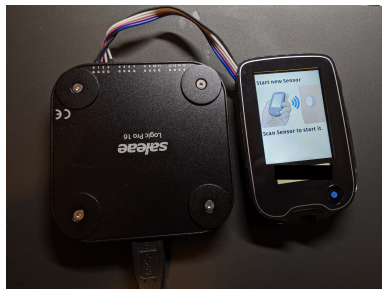
The screenshot shows the FortiGuard Labs website interface. At the top, there is a navigation bar with the FortiGuard Labs logo and links for Home, Zero Day, 2019, News / Research, Services, Threat Levels, Resources, and Search FortiGuard. Below the navigation bar, there is a section titled "At a glance" with a table of metrics:

VD Number	PC-VD-19-132
Date Discovered	See 03.2019
Risk	●●●●●
Impact	Date Manipulation

To the right of the table, there is a "Zero-Day Advisory" section with a warning icon and the title "Zero-Day Advisory". Below the title, it says "Fortinet Discovers Abbott FreeStyle Libre Sensor Unlock Code". A "Summary" section follows, stating: "Fortinet's FortiGuard Labs has discovered a NFC memory unlock code in certain Abbott FreeStyle Libre sensors." There is also a small image of a person in the background of the advisory section.

# 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



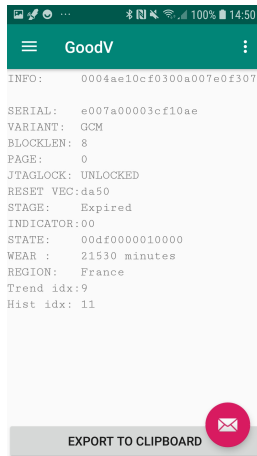
# Les étapes de notre démarche

- 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 rox_calledby_e0()  
R12_lo:1 <RETURN>  
undefined2 R15:2 addr XREF[1]: 526  
undefined1 R14_lo:1 len XREF[1]: 52  
rox_calledby_e0 XREF[4]: 1c72(+), 50  
FUN_51f4: 52  
fram_e0: fbc  
*****  
5256 0a 12 PUSH.W R10  
5258 b2 40 80 MOV.W #0x5a80, &MDTCTL  
5a 5c 01  
525e 5a 42 03 06 MOV.B &RFL3MINT_H, R10  
5262 c2 43 03 06 MOV.B #0, &RFL3MINT_H  
5266 3f 40 7a f8 MOV.W #0xf87a, addr  
526a 7e 40 93 00 MOV.B #0x93, R14  
*****  
zeroize trend record table and history table: we zeroize 0x93...  
LAB_526e XREF[1]: 5276(j)  
526e 8f 43 00 00 MOV.W #0, 0x0(addr)>trend_index  
5272 2f 53 INCD.W addr  
5274 7e 53 ADD.B #1, len  
5276 fb 23 JNE LAB_526e  
5278 e2 b2 c3 1c BIT.B #4, &DAT_1ccc3  
527c 16 26 JNC LAB_52aa  
527e 3f 40 66 f8 MOV.W #0x7866, addr  
5282 7e 40 09 00 MOV.B #0x9, len  
*****  
zeroize 0x09 words after the expiration indicator in the head...  
LAB_5286 XREF[1]: 528a(j)  
5286 8f 43 00 00 MOV.W #0, 0x0(addr)>DAT_fb86  
528a 2f 53 INCD.W addr  
528c 7e 53 ADD.B #1, len  
528e fb 23 JNE LAB_5286  
5290 c2 43 65 fe MOV.B #0, &fram_expirationindicator  
5294 df 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





# 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)

CRC 16 (2 bytes)

Index courant (1 octet)

Index historique (1 oc.)

Mesures courantes  
(16\*6 octets)

Historique (32\*6 octets)

Durée d'utilisation (2  
oc.)

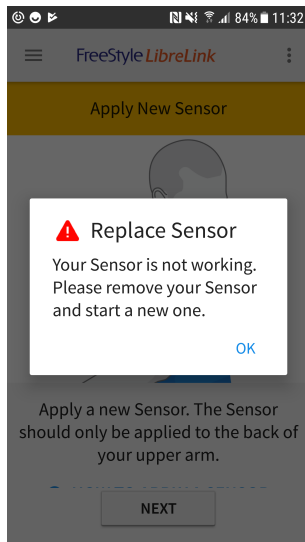
Inconnu (2 octets)

*Exemple : section des mesures*

# Assassinat d'un capteur

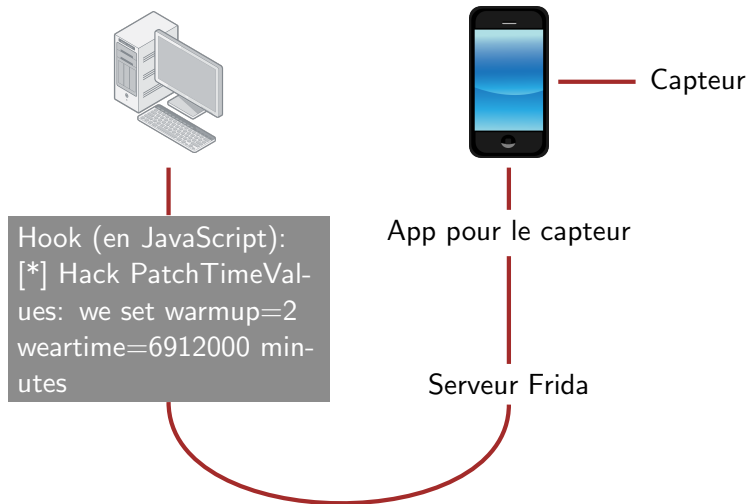
Deux façons de faire:

- 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
Réussusciter	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 !

Diabetes Symptoms (com.v1_4.B88FE0CB7322E72EB287D61F.com)	Detected	9Q288baal7836d3e6734073ae32c492b4540adeff778e6206ae76e8e4b3e437	Jul 26, 2020 12:47:27 AM
Signs of Diabetes (com.appman.signsofdiabetes)	Detected	d3e7cc939576a4d49d6cb31027c544fb0785ac4cb828767c0939181372990	May 22, 2020 9:55:02 AM - Unknown
What Is Diabetes (com.a72256693652b2e87a0d8ec7a.a29761526a)	Detected	41b477b2c9ad28f6eb6e105983bf129783536e1c0923a7e8509823910ab29c	May 20, 2020 10:52:21 AM
Signs of Diabetes (com.appman.signsofdiabetes)	Detected	h1Taa3041a97a38e4c21c520867d1e918e55ac8193990a55bf12c45hd1833873b	May 5, 2020 6:34:39 PM - Unknown
Triik Cegah Diabetes (com.TriikCegahDiabetes.sutriyanidroid)	Detected	6449d2a13198784cebc6530cf16c7d653543b6611c5c34db4ed11a05349a0	Apr 23, 2020 4:34:49 PM - Individual
Gejala Diabetes (com.GejalaDiabetes.mardianidroid)	Detected	#85bae1d0909a6e181c705a7c110a7e116c13036677d177b3a6f4a6f6d6	

# 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 @auresec @UYBHYS

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