



Capteur de glycémie connecté: les interdits

Axelle Apvrille (Fortinet)
Travis Goodspeed

Août 2020

Bonjour !



Axelle Apvrille

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

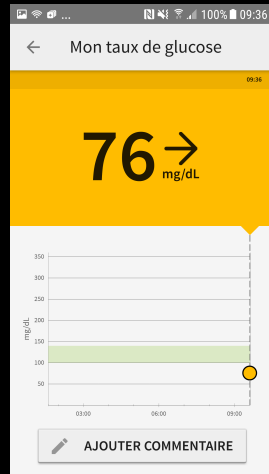
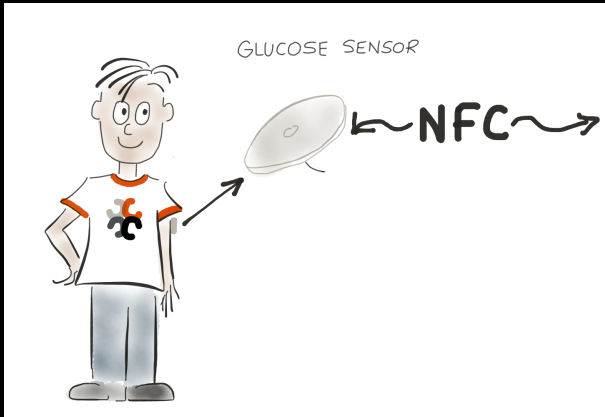


Travis Goodspeed

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



FreeStyle Libre: c'est vraiment utile !



Ça évite de devoir se piquer trop souvent

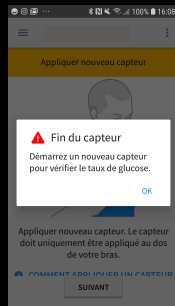


Cycle de vie d'un capteur

Monter le capteur



Appliquer le capteur



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

Expiration (14 j)



Contourner les limites

- 1 Expiration du capteur (démonstration)
- 2 Longévité du capteur (démonstration)
- 3 Durée d'activation (démonstration)
- 4 Zonage du capteur (pas de démonstration, mais même principe)

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

* Sortie officielle en Octobre 2018, mais toujours pas disponible en France en mars 2020. En Juin 2020, vendus en ligne, mais pas encore remboursés par la Sécurité Sociale.



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



Plan B pour la démo :P

```
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
```

EXPORT TO CLIPBOARD

Le capteur a expiré

```
Successfully erased tag
e007a00002b308e1 :))
```

EXPORT TO CLIPBOARD

Réinitialisation

```
INFO: 0004e108b30200a007e0f307
SERIAL: e007a00002b308e1
VARIANT: GCM
BLOCKLEN: 8
PAGE: 0
JTAGLOCK: UNLOCKED
RESET VEC:da50
STAGE: To Activate
INDICATOR:00
STATE: 00df000001640f
WEAR : 0 minutes
REGION: France
Trend idx:0
Hist idx: 0
```

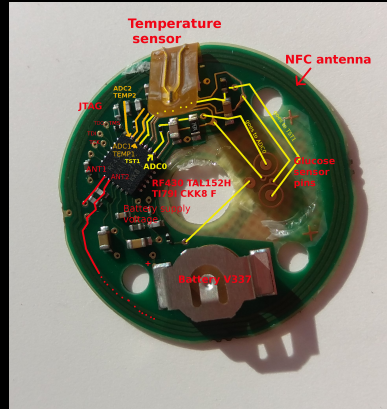
EXPORT TO CLIPBOARD

Prêt à être activé



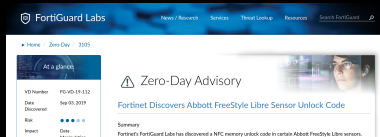
Les étapes de notre démarche

- 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)



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, problèmes de CRC

```
*****
*                               FUNCTION                               *
*****
undefined:row_calledby_e0()
undefined:R12_lo:1 <RETURN>
undefined2:R15:2 addr XREF[1]: 528
undefined1:R14_lo:1 len XREF[1]: 527
row_calledby_e0 XREF[4]: 1c72(*), 50
FRAM_51f4:52
fram_e0:fbcc

5256 0a 12 PUSH.W R10
5258 b2 40 80 MOV.W #0x5a80,&MOTCTL
5a 5c 01
525e 5a 42 03 06 MOV.B &RFP13MINT_H,R10
5262 c2 43 03 06 MOV.B #0,&RFP13MINT_H
5266 3f 40 7a fb MOV.W #0x187a,&addr
526a 7e 40 93 00 MOV.B #0x93,R14

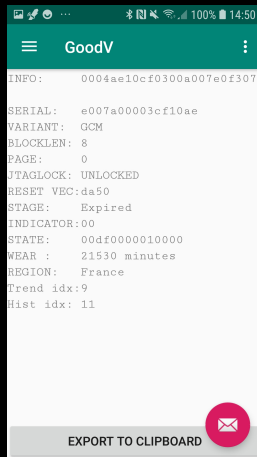
zeroize trend record table and history table: we zeroize 0x93...
LAB_526e XREF[1]: 5276(j)
526e bf 43 00 00 MOV.W #0,0x0(addr)=>trend_index
5272 2f 53 INCD.W addr
5274 7e 53 ADD.B #-1,len
5276 fb 23 JNE LAB_526e
5278 e2 b2 c3 1c BIT.B #4,&DAT_1ccc3
527c 16 28 JMC LAB_526a
527e 3f 40 66 fb MOV.W #0x1866,&addr
5282 7e 40 09 00 MOV.B #0x9,len

zeroize 0x09 words after the expiration indicator in the head...
LAB_5286 XREF[1]: 528e(j)
5286 bf 43 00 00 MOV.W #0,0x0(addr)=>DAT_fb66
528a 2f 53 INCD.W addr
528c 7e 53 ADD.B #-1,len
528e fb 23 JNE LAB_5286
5290 c2 43 65 fb 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, problèmes de CRC
- 5 Implémentation d'une appli Android



```
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
```

EXPORT TO CLIPBOARD



Pour en savoir (vraiment) plus

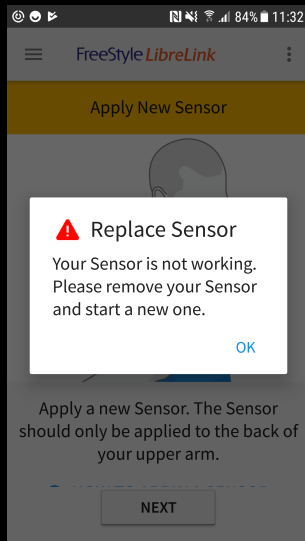
- Rapport complet de la sécurité du capteur de glycémie
- Video à Pass the SALT 2020



Démo: assassinat d'un capteur

Deux façons de faire:

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



Corruption mémoire



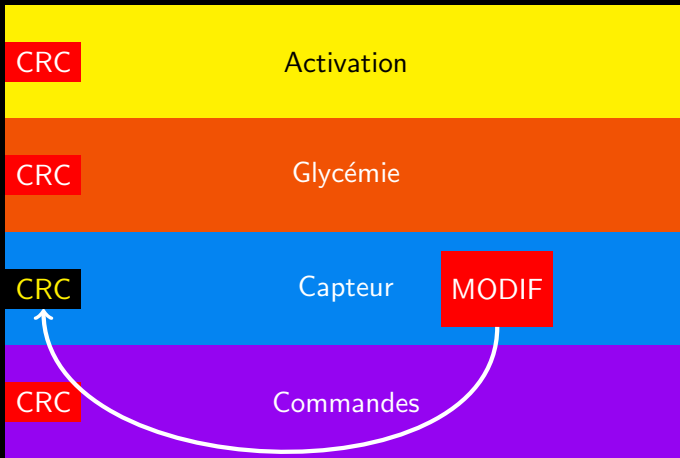
Comment ça marche ?



FRAM du capteur



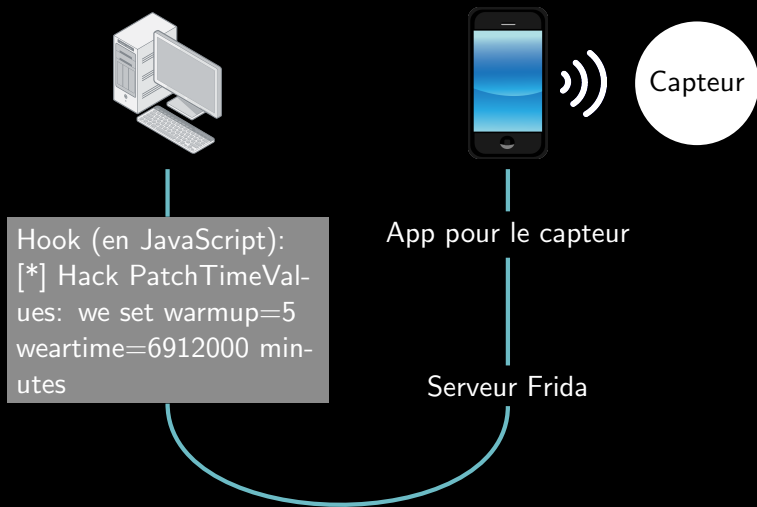
Comment ça marche ?



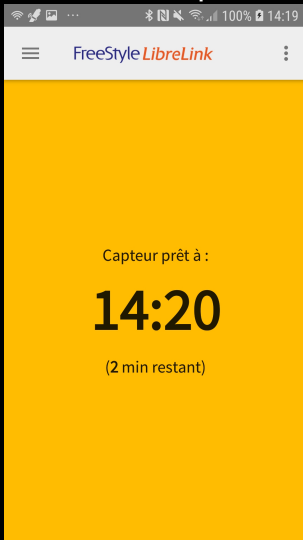
FRAM du capteur



Démo: hack de l'activation avec Frida



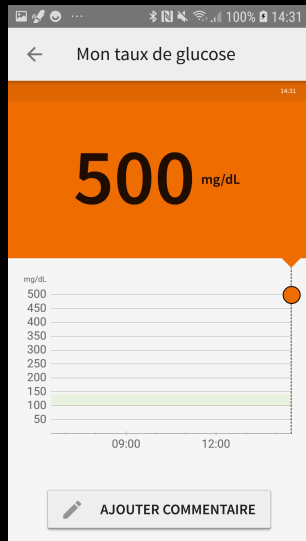
Les démos, parfois ça plante... ;P



Durée d'activation
modifiée à 2 minutes



Longévité de 4800 jours



Modification de la
glycémie



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

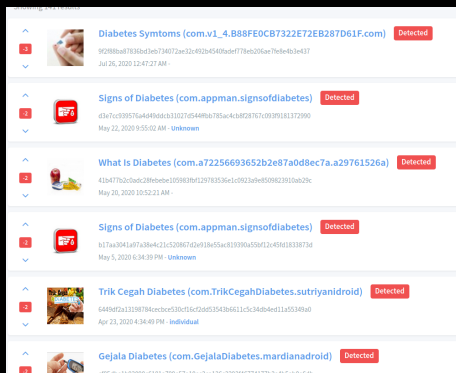
Vulnérabilités remontées au fabricant,
a priori ne sont plus présentes dans Libre 2.



Que ferait un attaquant ?

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

Les malwares “pour
diabétiques”, ça existe !



Références

- Security analysis of a Connected Glucose Sensor, Technical report
- GoodV Android application
- Readdump.py
- NFC exploitation with RF430RFL152 and 'TAL152, PoC || GTFO, 20:03



Merci pour votre attention, bon appétit !

Nous contacter :
@cryptax @travisgoodspeed

Merci particulièrement à
Contacts diabétiques anonymes et
@aamirlakhani @PagetPhil @TuxDePoinssise @aurelsec

