

Tuto RedSnowLite (MAC)

Conseil: Avant chaque étape, lire EN ENTIER ce qu'il faut faire dans cette étape, puis relire au fur et à mesure de votre avancement.

C'est un tuto relativement long mais il n'y a pas grand chose à faire, ce sont surtout des explications pour ne faire aucune erreurs.

Le problème majeur de cette manière de jailbreaker son ipod c'est que pour le rebooter, il faut répéter la dernière partie de ce tuto à savoir allumage de l'iPod. En effet, il est impossible que l'iPod démarre tout seul !

On peut bien sur l'utiliser normalement et le mettre en veille, mais c'est mieu (et moins chiant) de ne pas avoir à le rebooter.

Préparation:

Pour Réaliser ce Jailbreak nous allons avoir besoin:

- Avant tout, il faut installer libusb sur votre Mac, sinon l'ipod n'aura aucune chance d'être reconnu ! On peut télécharger libusb ici :

<http://www.ellert.se/PKGS/libusb-2008-09-27/10.5/libusb.pkg.tar.gz> Lien

- Un firmware Modifié appelé aussi CustomFirmware.

- L'application rslite qui joue le rôle d'interface entre l'iPod qui est en mode DFU (donc écran éteint) et le terminal de votre Mac.

- 4 fichier que l'on va envoyer dans l'iPod à l'aide de rslite.

Fichiers nécessaires ici --> <http://www.sosiphone.com/forum3G/viewtopic.php?t=4324>

Dézipper l'archive téléchargée et renommer le dossier en rslite (sauf si il s'appelle déjà rslite).

Dans ce dossier il y a TOUS les fichiers donc nous avons besoin.

Installation du CustomFirmware

1) Mettez votre iPodTouch 2G en mode DFU

--> 10 secondes Home+Bouton d'arrêt puis 10 secondes seulement le bouton home.

```
TomA ~ > cd Desktop/rslite
TomA ~/Desktop/rslite > ./rslite
rslite - by the iPhone Dev Team, 2009.
--THIS IS AN UNSUPPORTED TOOL--

Connecting...
Apple Mobile Device not found in Recovery or DFU
TomA ~/Desktop/rslite > |
```

Si l'ipod n'est pas en DFU ça donne ça au lancement de rslite.

Faire attention à ce qu' iTunes ne soit pas allumé, il est d'ailleurs conseillé de décocher la case 'Ouvrir iTunes à la connexion de cet iPod' mais aussi de tuer le processus iTunesHelper)

Pour cela ouvrez un Terminal (voir l'étape 2 pour ouvrir un terminal) et taper la commande

```
ps -u NomUtilisateur
```

Ensuite il faut repérer la ligne où se trouve le process iTunes Helper et noter son PID (deuxième numéro en début de ligne)

Enfin pour tuer ce processus il faut taper la commande

```
kill -KILL n°PID_Relevé
```

2) Il faut maintenant envoyer les fichiers que vous avez extraits des deux Firmwares dans l'étape 4.

À partir d'ici, tout ce passera dans une console (ou Terminal), pour l'ouvrir cliquez sur la loupe de spotlight (en haut à droite de l'écran) et tapez simplement Terminal à l'intérieur. Une fois les résultats affichés appuyez sur entrée pour le lancer.

Maintenant que vous êtes dans la consoles ne partez pas en courant, elle est gentille ! Il va falloir se déplacer dans le dossier rslite qui est sur votre bureau si vous m'avez écouté dans l'étape 1.

Dans le Terminal il faut taper (pas taper l'écran!):

```
cd Desktop/rslite
```

«cd» signifiant «Change Directory» et qui indique donc que l'on souhaite de déplacer dans le dossier rslite qui lui même est sur le bureau.

- Lancer rslite:

```
./rslite
```

- Envoyer le premier fichier:

```
!iBSS211.dfu
```

Ici l'écran devient blanc et rslite quitte.

- Re-lancer rslite:

```
./rslite
```

- Envoyer le deuxième fichier:

```
#pwn211ibss.txt
```

- Enfin le Troisième:

```
!iBSS221pwn.dfu
```

L'écran doit s'éteindre et redevenir blanc à cette étape (si ce n'est pas le cas, il faut recommencer l'envoi des fichier)

Ne pas fermer le terminal on en aura besoin juste après la restauration.

Voilà un aperçu de votre terminal à la fin de tout ça:

```

TomA ~/Desktop/rslite > ./rslite
rslite - by the iPhone Dev Team, 2009.
--THIS IS AN UNSUPPORTED TOOL--

Connecting...
Apple Mobile Device (DFU Mode)
CPID:8720 CPRV:10 CPFM:03 SCEP:01 BDID:00 ECID:          SRTG:[iBoot-240.4]
[DFU] !iBSS211.dfu
Executing: iBSS211.dfu
OK
TomA ~/Desktop/rslite > ./rslite
rslite - by the iPhone Dev Team, 2009.
--THIS IS AN UNSUPPORTED TOOL--

Connecting...

=====
::
:: iBSS for n72ap, Copyright 2008, Apple Inc.
::
::   BUILD_TAG: iBoot-385.22
::
::   BUILD_STYLE: RELEASE
::
::   USB_SERIAL_NUMBER: CPID:8720 CPRV:10 CPFM:03 SCEP:01 BDID:00 ECID:          SRNM:[          ]
::
=====

Entering recovery mode, starting command prompt
] [Recovery] #pwn211ibss.txt
] arm7_stop
] mw 0x9000000 0xe59f3014
] mw 0x9000004 0xe3a02a02
] mw 0x9000008 0xe1c320b0
] mw 0x900000c 0xe3e02000
] mw 0x9000010 0xe2833c9d
] mw 0x9000014 0xe58326c0
] mw 0x9000018 0xeaaffffe
] mw 0x900001c 0x2200f300
] arm7_go
] arm7_stop
[Recovery] !iBSS221pwn.dfu
Executing: iBSS221pwn.dfu
OK
TomA ~/Desktop/rslite >

```

- Il faut maintenant faire une restauration par iTunes qui, lorsque vous l'allumez détectera votre ipod en mode récupération (si l'écran est blanc). Maintenez donc la touche Alt enfoncé et choisissez le CustomFirmware qui doit se trouver dans le dossier rslite sur le bureau (et oui, toujours lui!)

À la fin de la restauration, l'ipod ne peut pas s'allumer tout seul :(Il faut donc l'aider un peu.

Allumage de l' iPod

- Passer en mode DFU (comme expliqué précédemment. l'écran reste noir mais c'est pas grave il faut quand même appuyer sur les bouton!)

- Si vous avez fermé le Terminal il faut se rendre dans le dossier rslite:

```
cd /Desktop/rslite
```

- Lancer rslite:

```
./rslite
```

- Envoyer le premier fichier:

```
!iBSS211.dfu
```

Ici l'écran devient blanc et le programme quitte.

