Forum:Hack Forums

Thread: [TuT] Downgrade iOS 4.3.5 to 4.3.3 WITHOUT SHSH Blobs + JailBreak! [TuT]

Maurice Moss - *September 24, 2011, 9:50 pm*

Hello all! My friend has asked me to fix his iPod and give him an untethered jailbreak, but I told him I couldn't do that with iOS 4.3.5 since there is no untethered jailbreak available. I told him I could possibly try and downgrade to 4.3.3 and I have managed to do it. Being this is a brand new iPod Touch 4G and Apple is not signing SHSH blobs, people have been having trouble or not be able to downgrade their devices.

Note: This is a TETHERED jailbreak ONLY.

Before you continue, by doing this you agree that I have no responsibility for what you do to your device.

Step 1: Gather your downloads.

You will need:
iOS 4.3.3 Download

Redsn0w 0.9.6rc15 Download

iREB Download

TinyUmbrella Download

iTunes 10.4 (or newer) Download

Step 2: Enter pwned DFU Mode

Start up iREB.

Click on your device.

Follow DFU steps.

After a few moments, your device will be in a pwned DFU state.

Step 3: Restore on iTunes

Open up TinyUmbrella and click on "Start TSS Server"

If you had iTunes open, TinyUmbrella will close it. Re-open it and you should get the message "iTunes has detected an iPod in recovery mode. You must restore this iPod before it can be used with iTunes."

Click on OK.

If you're on a PC, hold down left shift, then click on restore. If you're on a mac, hit control, then click on restore.

Browse for the 4.3.3 IPSW, click on "Open" then click on "Restore".

Your iDevice should start to restore.

When it's done, you'll get the recovery mode error again. Don't worry. (You may get Error 37 too. Disregard this error.)

Step 4: Jailbreak

Open up Redsn0w and click on "Browse" Locate the 4.3.3 IPSW.

Click on "Next". If you've ever used redsn0w before, you'll have to put your device into DFU mode manually. In this case, your iDevice is already in DFU mode and the jailbreak process will start immediately.

Check your options for the jailbreak you would like, then click next. The jailbreak process will start.

On your iDevice, it may get frozen on "Installing Bundles". Hold down home + power button to reset it, then proceed to step 5.

Step 5: Boot up iDevice

After the jailbreak process on your iDevice has finished, re-open redsn0w if you have closed it, otherwise just click on "back".

Now this time, only check "Just boot tethered right now."

Go through the same steps and your iDevice should boot up fine.

After it has booted up, you'll see the Apple logo and the progress bar. At this point it is finishing the 4.3.3 restore and it will show the recovery mode screen. Open up iTunes to set up the iDevice.

Congratulations. You're now back on iOS 4.3.3.

Credits go to everyone that made the programs. Credits go to me for this method and writing tutorial.

Note: Any time you need to turn off/restart your iDevice, you will need to open up redsn0w and "Just boot tethered right now.", otherwise your iDevice will be stuck in a DFU mode.

Thank you for reading! Please don't hesitate to PM if you have any questions.

Son of Sparta - *September 24, 2011, 11:15 pm*
Nice one, would be useful for many of the needy people.

FeaR ™ - *September 24, 2011, 11:18 pm*
Don't use redsnow to jailbreak on 4.3.3 just use jailbreakme.com
Good tutorial tho

Maurice Moss - *September 25, 2011, 11:38 am*
(Sep 24, 2011 11:18 PM)Tyga™ Wrote: [CITE] Don't use redsnow to jailbreak on 4.3.3 just use jailbreakme.com
Good tutorial tho
You have no choice. You need the jailbreak with redsn0w to then be able to use the tether boot in order to turn on your iPod. If you want, you can use jailbreakme.com afterwards but the jailbreak will still be tethered either way.

NOOB5029 - *September 25, 2011, 12:11 pm*
? wait wouldnt it be UNtethered...? >_> ugh i never did learn the differences:

Maurice Moss - *September 25, 2011, 12:57 pm*
(Sep 25, 2011 12:11 PM)NOOB5029 Wrote: [CITE] ? wait wouldnt it be UNtethered...? >_> ugh i never did learn the differences:
Untethered means you don't need a program to turn on your iDevice.

Tethered means you'll need a program in order to start the jailbreak and your iDevice.

Grin - *September 25, 2011, 2:51 pm*
Great tutorial. Did you find this out yourself? I found out a method similar to thus one back in the 3.1.3 fws. I helped my friend jailbreak it without any tutorials. Simple 20$
Took some trial and error, though.

Maurice Moss - *September 25, 2011, 3:27 pm*
(Sep 25, 2011 02:51 PM)Grin Wrote: [CITE] Great tutorial. Did you find this out yourself? I found out a method similar to thus one back in the 3.1.3 fws. I helped my friend jailbreak it without any tutorials. Simple 20$
Took some trial and error, though.
I discovered this myself while trying some other tutorial I found, which didn't work.

Breakbeat Junkie - *September 25, 2011, 3:34 pm*
Testing this now. My iPhone has been f*cked for over 4 hours now, I hope this works :>

I'll edit this post.

Edit: Doesn't work for me.
Getting 1013 error.

AnthonyWasH3r3 - *September 25, 2011, 4:45 pm*
Running jailbreakme over a tethered 4.3.3 jailbreak SHOULD make it untethered. Have you gave that a try?

Tacitus - *September 25, 2011, 5:24 pm*
Would the downgrade steps work on a iPad 2 as well?

Maurice Moss - *September 25, 2011, 7:22 pm*
(Sep 25, 2011 05:24 PM)Tacitus Wrote: [CITE] Would the downgrade steps work on a iPad 2 as well?
It may. I did this on a iPod Touch 4G.

(Sep 25, 2011 04:45 PM)AnthonyWasH3r3 Wrote: [CITE] Running jailbreakme over a tethered 4.3.3 jailbreak SHOULD make it untethered. Have you gave that a try?
I have, but it was still tethered.

(Sep 25, 2011 03:34 PM)?eborn Wrote: [CITE] Testing this now. My iPhone has been f*cked for over 4 hours now, I hope this works :>

I'll edit this post.

Edit: Doesn't work for me.
Getting 1013 error.
Did you start the TinyUmbrella TSS server?

Breakbeat Junkie - *September 26, 2011, 4:38 am*
(Sep 25, 2011 07:22 PM)?lash Wrote: [CITE] Did you start the TinyUmbrella TSS server?
Of course I did.

Maybe you could help me over TV? Lol.

Trihunter3 - *October 2, 2011, 7:15 pm*
i got the 1013 error also, basically what i did was this:

I went and just jailbroke it with redsnow,
Booted it,
jailbroke it again
booted it, and it worked....

Now i am trying to use snowbreese to hactivate it.

black111 - *October 10, 2011, 3:21 pm*
nice tutorial and all is works perfectly this is the first working tutorial about downgrading im searching about this from 1 week ago nice one !!!! and thx a lots....

PedroDJ - *October 11, 2011, 2:17 am*
I have tryed to downgrade from 4.3.5 to 4.3.3 without SHSH blobs without lucky: i have tryed this tutorial and this one https://hackforums.net/showthread.php?tid=1653547

Regards