

Forum:[Hack Forums](#)

Thread: [How to CORRECTLY downgrade/upgrade your iDevice's firmware](#)

D3xus - September 30, 2011, 5:07 am

Written by me for the n00bs... this is as easy as it comes so pay attention! ?

You need some things for this to work. An iPod touch, iPhone or iPad that is jailbroken.

SHSH blobs for a specific firmware. To find out what SHSH blobs you have, refer to below.

TinyUmbrella, download it from <http://thefirmwareumbrella.blogspot.com>

Note, if you are doing this tutorial with an iPod 2g or an iPhone 3g, you do not need TinyUmbrella. They do not need to have upgrades and downgrades be confirmed by an Apple server. For the sake of the tutorial, I am doing it anyways.

iReb; <http://ih8sn0w.com>

To find out what SHSH blobs you have, first unlock your iDevice and load up Cydia. Then, at the VERY top you should see something that says 'SHSH: 'and a list of different versions of iOS.

Look at the below screenshot if you're still unsure.

Click me to see the picture. [\(Click to View\)](#)

[IMG]<http://i1126.photobucket.com/albums/l601/DXTechHelp/18fc9d31.jpg>[/IMG]

Ok then. Now that we're ready to roll, double click on TinyUmbrella and load it.

The device I'm using is in recovery mode for later on in the tutorial, so it will appear that way in the screeny.

Click me to see the picture. [\(Click to View\)](#)

When it has booted up, connect your iDevice to the computer. TinyUmbrella will see it in addition to iTunes.

For restoring purposes, you have to put your iPhone into what is known as pwned DFU mode (short for Damn I Fucked Up.) This is done by doing the following steps. You will need the iReb program that I mentioned earlier to pull Pwned DFU mode off.

- 1) Turn the iPhone completely off.
- 2) Hold the power button for 2 seconds until you see the Apple logo.
- 3) Hold down the Power button and home button for 10 seconds, or until your computer de recognizes the device (whichever comes first.)
- 4) At that point in time, release the power button, but keep holding the home button until your computer sees it in recovery mode.

Click me to see the picture. [\(Click to View\)](#)

5) Load up iReb and then in the main interface, select the iDevice that is currently in regular DFU mode. I'm using an iPhone 3G, so I'm gonna be using that.

When you load it, it should look like this.

Click me to see the picture. [\(Click to View\)](#)

Select the iDevice that you're using and then it should detect it in DFU mode and exploit it using either limer1n, st4aksauce or another bootrom exploit.

We will now use a pre-jailbroken firmware, custom made by a program such as sn0wbreeze or PwnageTool. I will be using one that I made already. You need to make your own with the right programs.

When you've gotten the firmware, and when your iPhone is in pwned DFU mode, hold the Shift key on your keyboard (in Windows, if you're on a Mac, hold Control or Alt) and click Restore.

Click me to see the picture. [\(Click to View\)](#)

You will then be prompted to browse to where you downloaded or created the custom firmware. Select that firmware.

Click me to see the picture. [\(Click to View\)](#)

Then you're done. iTunes will take care of the rest and you'll be going down, or up, in iOS software. If you run into problems, just ask me or another iDevice Lover.

Døn - September 30, 2011, 6:31 am

Looks like a great tut but the pictures are not working

MaNiFesTox - October 1, 2011, 8:54 pm

(Sep 30, 2011 05:07 AM)D?xus Wrote: [\[CITE\]](#) Written by me for the n00bs... this is as easy as it comes so pay attention! ?

You need some things for this to work. An iPod touch, iPhone or iPad that is jailbroken.

SHSH blobs for a specific firmware. To find out what SHSH blobs you have, refer to below.

TinyUmbrella, download it from <http://thefirmwareumbrella.blogspot.com>

Note, if you are doing this tutorial with an iPod 2g or an iPhone 3g, you do not need TinyUmbrella. They do not need to have upgrades and downgrades be confirmed by an Apple server. For the sake of the tutorial, I am doing it anyways.

iReb; <http://ih8sn0w.com>

To find out what SHSH blobs you have, first unlock your iDevice and load up Cydia. Then, at the VERY top you should see something that says 'SHSH: 'and a list of different versions of iOS.

Look at the below screenshot if you're still unsure.

Click me to see the picture. [\(Click to View\)](#)

[IMG]<http://i1126.photobucket.com/albums/l601/DXTechHelp/18fc9d31.jpg>[/IMG]

Ok then. Now that we're ready to roll, double click on TinyUmbrella and load it.

The device I'm using is in recovery mode for later on in the tutorial, so it will appear that way in the screeny.

Click me to see the picture. [\(Click to View\)](#)

When it has booted up, connect your iDevice to the computer. TinyUmbrella will see it in addition to iTunes.

For restoring purposes, you have to put your iPhone into what is known as pwned DFU mode (short for Damn I Fucked Up.) This is done by doing the following steps. You will need the iReb program that I mentioned earlier to pull Pwned DFU mode off.

- 1) Turn the iPhone completely off.
 - 2) Hold the power button for 2 seconds until you see the Apple logo.
 - 3) Hold down the Power button and home button for 10 seconds, or until your computer de recognizes the device (whichever comes first.)
 - 4) At that point in time, release the power button, but keep holding the home button until your computer sees it in recovery mode.
- Click me to see the picture. [\(Click to View\)](#)

5) Load up iReb and then in the main interface, select the iDevice that is currently in regular DFU mode. I'm using an iPhone 3G, so I'm gonna be using that.

When you load it, it should look like this.

Click me to see the picture. [\(Click to View\)](#)

Select the iDevice that you're using and then it should detect it in DFU mode and exploit it using either limera1n, st4ksauce or another bootrom exploit.

We will now use a pre-jailbroken firmware, custom made by a program such as sn0wbreeze or PwnageTool. I will be using one that I made already. You need to make your own with the right programs.

When you've gotten the firmware, and when your iPhone is in pwned DFU mode, hold the Shift key on your keyboard (in Windows, if you're on a Mac, hold Control or Alt) and click Restore.

Click me to see the picture. [\(Click to View\)](#)

You will then be prompted to browse to where you downloaded or created the custom firmware. Select that firmware.

Click me to see the picture. [\(Click to View\)](#)

Then you're done. iTunes will take care of the rest and you'll be going down, or up, in iOS software. If you run into problems, just ask me or another iDevice Lover.

well said and well informed i like it and its organise well great job bro

Grin - October 1, 2011, 11:15 pm

Very well organized and informative. Will do many people favors.

Grin - October 14, 2012, 8:02 pm

iOS 6 has the reresstore option, so it could be different.

Good fundamental though.

Genius1223 - October 14, 2012, 8:32 pm

This is an awesome guide.

Hope Users will refer to this guide before asking now.

Grin - October 14, 2012, 8:40 pm

Not a chance! They won't bother... :/

Genius1223 - October 14, 2012, 9:00 pm

Yep.

like 10% chance people may read it. xD

If this section didnt have you guys, i would have been a dead section

Grin - October 14, 2012, 9:02 pm

yEA, but that's in the way bottom, and no one searches.

Genius1223 - October 14, 2012, 9:25 pm

Thats why i was asking for some threads to be stickied as in Important threads sticky thing.

Not the one by paying money but the one which technically solves 90%user problems in the thread itself.

Grin - October 14, 2012, 9:27 pm

He did pay for it for a time being, then obv...it expired.

Actually devi001 paid for it.

Grin - October 14, 2012, 9:43 pm

No, it's like two weeks or something for \$20.

Genius1223 - October 14, 2012, 10:50 pm

Stickies are fking costly.

So basically it should be stickied for free as the thread will enlighten all the members on the forum but meh I am just a guy whose voices wont matter :p

Grin - October 15, 2012, 1:10 pm

No. I agree with you and so did a lot of people back then.

D3xus - October 15, 2012, 1:40 pm

I could revamp my thread into a mega guide or make a new thread entirely if I get some help making it. It would have to be MASSIVE.

Grin - October 15, 2012, 4:25 pm

It would have to be massive, I can help if you need.

Genius1223 - October 15, 2012, 8:07 pm

I can help you.

Give me a topic to cover and I'll do it.

Lets do this and get an AIO thread ;)

jman1094 - October 15, 2012, 9:44 pm

Would I be able to save a SHSH blog on my iPhone and send it to a friend who upgraded to iOS 6 in order for him to downgrade to 5.1.1 on his iPhone?

Grin - October 15, 2012, 10:22 pm

(Oct 15, 2012 09:44 PM)jman1094 Wrote: [\[CITE\]](#) Would I be able to save a SHSH blog on my iPhone and send it to a friend who upgraded to iOS 6 in order for him to downgrade to 5.1.1 on his iPhone?

It's kind of vague...what iphone? lol

jman1094 - *October 15, 2012, 10:38 pm*

my iPhone 4 is jailbroken on iOS 5.1.1

my friends iPhone 4 isn't jailbroken but is on iOS 6

Can I use my SHSH blob on his iPhone?

Grin - *October 15, 2012, 10:39 pm*

No you can't share SHSH blobs if that's what you're asking.

jman1094 - *October 15, 2012, 10:40 pm*

Ok. that answers my question, thank you.

Grin - *October 15, 2012, 10:42 pm*

No problem, any more problems feel free to make a thread. I'll get to it.