Tegra3 Guide: nvflash NEXUS 7 (and Transformer Jellybeans)

Introduction

NOTE: As always, the files are non-redistributable! (This only applies to the image itself and wheelie.)

Those with the Nexus 7 or who upgraded to Jellybean before getting nvflash access - we did not forget about you!

This guide will walk you through the process of acquiring nvflash access to your tablet. Note that this has only been tested on TF201, TF300, TF700 and Nexus 7 (Wi-Fi + 3G)!

As part of the process of gaining this access you will need to flash the AndroidRoot patched custom bootloader. However, flashing the bootloader is a potentially very risky activity so please think carefully before you proceed!

As part of undertaking this guide you disclaim AndroidRoot and its members of all liability or responsibility for any damage incurred. By performing the following steps you undertake all risks thereof.

Please note that this procedure is an advanced process and should only be completed by competent users.

The AndroidRoot Patched Bootloader

The current AndroidRoot.mobi bootloader versions are

- Transformer Prime TF201: **10.4.2.15 (INCOMPATIBLE WITH HAIRY BEAN)**

- Transformer TF300: **10.6.1.15.3**

- Transformer TF700**: 10.6.1.14.4**

- Nexus 7 (2012): **4.13**

Prerequisites

1. An unlocked TF201, TF300, TF700 or Nexus 7 (2012) Wi-Fi & 3G tablet
2. Working fastboot binary & all necessary drivers
3. The nvflash binary from NVIDIA (See Downloads)
4. Nerves of steel!

Generating your nvflash blob files

To gain access to nvflash you will need to generate nvflash blob files which will allow you to authenticate with the APX mode on device.

To begin please download the file suitable for your OS and tablet from the download section.

When you have downloaded the pack for your device, you will need to reboot your device into fastboot mode. You can do this by rebooting the device and holding the volume down key until "Checking for RCK image" appears, at this stage do nothing until the boot menu loads. Once you are at the boot menu please enter fastboot mode (if the device is not already in fastboot mode). The exact procedure for entering fastboot mode differs between different devices.

(Please note that for transformer tablets the fastboot command might require the option "-i 0x0b05".)

Now that you are in fastboot mode please run the following command to flash the AndroidRoot recovery image:-

> $ fastboot flash recovery flatline_device.img

Please ensure flashing succeeds before continuing this guide. A blue bar will be shown on screen indicated that flashing succeeded.

After the flash process has completed you will need to reboot your device into recovery. It is important that you reboot completely rather than directly enter recovery. If you don't there is a risk that the process can fail.

Once your device has booted into recovery, select the "Wheelie" menuitem in the "Advanced" item, accepting the warning if you wish to continue. At this stage you will need to select "Step 1: Flash AndroidRoot BL" which will flash the AndroidRoot custom bootloader.

The device will power off. Power the device back on and allow it to boot normally into Android. Once the device has fully booted please reboot the device back into recovery mode.

Once your device has booted into recovery again, you need to select "Step 2: Generate wheelie blobs" from the Wheelie menu in Advanced.

This will generate your nvflash blobs and if a wifi connection is able to be initialised, it will upload the blobs for safe keeping to the AndroidRoot webserver (there is nothing confidential about your encrypted nvflash blobs). After blob generation is complete, please follow the on the screen prompt to retrieve your blobs from the /data partition. (This will either be "adb pull /data/media/AndroidRoot" or "adb pull /tmp/AndroidRoot".)

** **You absolutely must keep these files in triplicate copies - they are your life-line** **

Please note that the blob generation process can take a fair amount of time so feel free to go grab a tea or coffee at this stage. Your device probably hasn't crashed!

Accessing nvflash

Finally, you will now be able to access nvflash using wheelie. To do this please reboot your tablet into APX mode by holding down the volume up key during the reboot process. If successful the screen should remain blank and be detected over USB by your computer as an NVIDIA APX mode device. **Windows Note:** This will probably not work on Windows 8 without entering test mode. We are not aware of any fully signed APX Mode driver.

To "bootstrap" into nvflash using wheelie simply run the following command:-

> $ wheelie --blob blob.bin

If successful your device will boot into nvflash mode and the bootloader screen will appear on the device.

WARNING: If you run the following command it will boot your device into regular android. This is listed as an *EXAMPLE*. Run the commands in "What Next?" section first.

From this point you will be able to use nvflash as normal by running commands such as the following to continue booting your device:-

```
$ nvflash --resume --go
```

What Next?

Good news! You have acquired nvflash access so what should you do next?

We strongly recommend that absolutely everyone who obtains nvflash access runs the following command:-

Transformer Devices:

$ nvflash --resume --rawdeviceread 0 2944 bricksafe.img

Nexus 7:

$ nvflash --resume --rawdeviceread 0 2688 bricksafe.img

This is a very important back-up file which is to be stored safely along with your nvflash blob files.

** Failure to make this back-up file will lead to support being withheld if you brick your device. You have been warned. **

For the ASUS Transformer series devices, the following backups are recommended:

```
$ nvflash --resume --read 14 factory-config.img
```

```
$ nvflash --resume --read 7 unlock-token.img
```

```
Store these files securely with the blob data and bricksafe.img
```

For Nexus 7, we recommend backing up the following partitions:

```
$ nvflash --resume --read 5 eks.img
```

```
$ nvflash --resume --read 13 factory-config.img
```

> $ nvflash --resume --read 14 mda.img

Downloads

- NVFlash: Windows (http://www.androidroot.mobi/download/nvflash-tools-win32.zip) | Linux (http://www.androidroot.mobi/download/nvflash-tools-linux.tar.bz2)

- TF201: Download (http://www.androidroot.mobi/download/flatline_tf201.img)

- TF300: Download (http://www.androidroot.mobi/download/flatline_tf300.img)

- TF700: Download (http://www.androidroot.mobi/download/flatline_tf700.img)

- Nexus 7: Download (http://www.androidroot.mobi/download/flatline_grouper.img)

- Drivers: Windows (http://forum.xda-developers.com/showthread.php?t=1426502)

- Drivers TF700: Windows (http://www.androidroot.mobi/download/Universal_Naked_Driver_0.7_tf700.zip) (Patched Universal Naked Driver (http://forum.xda-developers.com/showthread.php?t=1426502)) (May or may not work! We recommend using Linux.)

Credits

In alphabetical order the entire AndroidRoot.mobi team: Bumble-Bee, IEF, kmdm, lilstevie & RaYmAn.

Our beta-testers for risking their devices so that you don't have to (in no particular order):

- XpLoDWilD (TF300, TF700)

- Dees_Troy (TF700)

- AndroidRoot Team ;)

We would also like to take this opportunity to thank ASUS & Google for providing the ability to unlock the Transformer Prime and to further state that **DRM is not compromised** since the DRM keys have already been erased from the device during the unlock process and our work can only be used on an unlocked device.

Finally we would like to thank the Clockwork Mod Recovery developers for the recovery platform that flat-line is based on