

DSiWare Downgrade

Plailect edited this page Oct 20, 2016 · 79 revisions

If you are on 11.0.0 or 11.1.0, you must follow this guide to downgrade your NATIVE_FIRM using DSiWare and a second 3DS which has already has a Custom Firmware installed on it in order to dump and restore your NAND.

If you are below 11.1.0 on either device, then you should do the ctr-httpwn steps (when prompted) on each device under 11.1.0 to allow you to System Transfer with them.

This takes advantage of an oversight which allows DSiWare titles to read and write anywhere in NAND.

This is a currently working implementation of the "FIRM partitions known-plaintext" exploit detailed [here](#).

This guide will assume the CFW 3DS is running arm9loaderhax and was setup with this guide, but will work (with slight modifications such as doing all SysNAND steps on EmuNAND) on systems running an EmuNAND. Note that the terms EmuNAND and RedNAND refer to slightly different implementations of [the same concept](#).

This exploit requires you to [System Transfer](#) from a CFW 3DS to a stock 3DS as part of the steps. System Transfers will work in the following directions *only*:

- New 3DS -> New 3DS
- Old 3DS or 2DS -> Old 3DS or 2DS
- Old 3DS or 2DS -> New 3DS

3DS #1's NNID will be stuck on 3DS #2 unless you either system transfer back or call Nintendo! (details in the instructions)

Both systems MUST be from the same region.

System Transfers can only be performed once a week.

What you need

- Two 3DS systems
 - **3DS #1**: the 3DS running some kind of custom firmware (arm9loaderhax or some form of EmuNAND/EmuNAND) *on the latest version*
 - **3DS #2**: the 3DS on stock firmware *on 11.0.0 or 11.1.0*
- Purchase one of the following exploitable DSiWare games (a pirated copy of the game will **not** work) on **3DS #1**
 - **Fieldrunners**: Works for **USA + EUR** (never released for JPN)
 - **Legends of Exidia**: Works for **USA + EUR** (JPN title pulled from eShop)
 - **Guitar Rock Tour**: Works for **EUR Only** (game has been pulled in all regions, you must have installed it already)
- The exploited save for your game and region:
 - **Fieldrunners USA Region**: [public.sav](#)
 - **Fieldrunners EUR Region**: [public.sav](#)
 - **Guitar Rock Tour EUR Region**: [public.sav](#)
 - **Legends of Exidia ALL Regions**: [public.sav](#)
- The latest release of [3DSident](#)

Pages 33

[Home](#)
[FAQ](#)

[OTP Info](#)
[NAND Size](#)

Get Started

[Updating A9LH](#)
[Region Changing](#)

[Troubleshooting](#)

[Donations](#)
[Credits](#)

Clone this wiki locally

<https://github.com/Plailect/>

- The latest release of [FBI](#)
- The latest version of [Universal Inject Generator](#)
- The Homebrew [Starter Kit](#)
- The release of dgTool corresponding to **3DS #2's** version:
 - 11.0.0 Compatible [Release](#)
 - 11.1.0 Compatible [Release](#)
- The firmware zip corresponding to the device and version of **3DS #2**:
 - [New 3DS 11.0.0 to 10.4.0](#)
 - [Old 3DS 11.0.0 to 10.4.0](#)
 - ~
 - [New 3DS 11.1.0 to 10.4.0](#)
 - [Old 3DS 11.1.0 to 10.4.0](#)
- If **3DS #2** is below 11.1.0, you will *also* need the following
 - The latest release of [ctr-httpwn](#)
- If **3DS #2** is on 11.1.0, you will *also* need the following
 - Download a legitimate copy of **Steel Diver: Sub Wars** (the game is free, but any copy of the game not from the eShop will **not** work) on **3DS #1**
 - The latest release of [steelhax](#)

Instructions

Section I - Prep Work

1. Create a folder named `files9` on the root of **3DS #1's** SD card if it does not already exist
2. Use a [save manager](#) to backup any saves you care about on **3DS #2** (it will be formatted!)
3. Copy `public.sav` to the root of **3DS #1's** SD card
4. On **3DS #1**, hold Start on boot to launch Hourglass9
5. If you do not have `NANDmin.bin` or `NAND.bin` on your computer already, do the following:
 - Go to SysNAND Options, then SysNAND Backup/Restore, then backup (**min size**) SysNAND to `NAND.bin`
 - Press (Select) on the main menu to eject your SD card, then put it in your computer
 - Copy `NAND.bin` and `NAND.bin.sha` from the `/files9/` folder on your SD card to a safe location; make backups in multiple locations; this backup will save you from a brick if anything goes wrong in the future (**Your backup should match one of the sizes on [this](#) page; if it does not, you should delete it and make a new one!**)
6. Press (Select) on the main menu to eject **3DS #1's** SD card, then put it in your computer
7. Put **3DS #2's** SD card into your computer
8. **Backup every file on both 3DS's SD cards to two separate folders on your computer (keep track of which is which)!**
9. Reinsert each SD card back into their corresponding 3DS
10. Press (Start) to reboot

Section II - Installing the save

1. Purchase one of the following exploitable DSiWare games (a pirated copy of the game will **not** work)
 - **Fieldrunners**: Works for **USA + EUR**
 - **Legends of Exidia**: Works for **USA + EUR**
 - **Guitar Rock Tour**: You must have already purchased this for **EUR**
2. Launch FBI on **3DS #1**
3. Navigate to `SD`
4. Press (A) on `public.sav` and copy it
5. Press (B) to get back to the main menu
6. Navigate to `TWL NAND -> title -> 00030004`
7. Navigate to the folder for your game and region:
 - **Fieldrunners USA Region**: `4b464445 -> data`

- **Fieldrunners EUR Region:** `4b464456` -> `data`
 - **Legends of Exidia USA Region:** `4b4c4545` -> `data`
 - **Legends of Exidia EUR Region:** `4b4c4556` -> `data`
 - **Guitar Rock Tour EUR Region:** `4b475256` -> `data`
8. Press (A) on the existing `public.sav` and delete it
 9. Press (A) on the current directory and paste `public.sav`
 10. Press (B) to get back to the main menu
 11. Press (Start) to exit
 12. Launch your DSiWare game on **3DS #1**
 13. Test if the save is functional
 - **Fieldrunners:** Touch the 'Scores' button at the main menu
 - **Legends of Exidia:** After pressing (A) or (Start) at the two title screens, select the first save slot and press continue
 - **Guitar Rock Tour:** Scroll down and go to High-Scores -> Drums -> Easy
 - If your game has an error about `boot.nds` , **then the exploit has been successful**
 - If your game behaves normally and does not give you this error, then you should stop and figure out what went wrong
 - If you get a black screen, [follow this troubleshooting guide](#)

Section III - steelhax

This section is only required if 3DS #2 is on 11.1.0.

This will allow you to enter the homebrew launcher after the System Transfer.

1. Copy the `steelhax-installer` folder from the steelhax zip to the `/3ds/` folder on **3DS #1's** SD card
2. Reinsert your SD card into your 3DS
3. Ensure that **Steel Diver: Sub Wars** does not have any updates installed using System Settings:
 - Go to "Data Management", then "Nintendo 3DS", then "Downloadable Content"
 - Select **Steel Diver: Sub Wars**, then select "delete"
 - Exit the System Settings
4. Launch **Steel Diver: Sub Wars**
 - Do not update the game
5. Press (A) to continue, then create / select a Mii
6. Exit the game
7. Launch the homebrew launcher on **3DS #1**
 - If it is an arm9loaderhax installed device, you can do that with [hblauncher_loader](#)
8. Launch steelhax installer
9. Press (A) to continue
10. Press (A) to confirm **Steel Diver: Sub Wars's** version
11. Press (A) to confirm **3DS #1's** system version
12. Press (Start) to exit the installer
13. Press (Start) to open the homebrew launcher exit menu
14. Press (X) to Return to Home Menu (no reboot)
 - You may get an "Error has occurred" message with the option to continue. This is fine, just hit (A)
15. Launch **Steel Diver: Sub Wars** to test the exploit
 - Do not update the game
 - The save game may be corrupted
 - Do not press "ok" to delete the corrupted save data, just exit with the home button
 - If you do press "ok" by mistake, you will have to recreate the Mii
 - Redo the installation starting with the homebrew launcher
 - This can take many tries
 - If it is successful, the device will boot into the homebrew launcher

16. Once you are in the homebrew launcher successfully, launch steelhax installer
17. Press (A) to continue
18. Press (A) to confirm **Steel Diver: Sub Wars's** version
19. This time, change the version to match **3DS #2's** system version
 - Even though you will be downgrading its firmware, you should still select the version it is on now
20. Copy the *contents* of the `starter.zip` to the root of **3DS #2's** SD card, then put the SD card back into **3DS #2**

Section IV - ctr-httpwn

This section is only required if 3DS #2 is under 11.1.0.

This will allow you to system transfer on versions other than the latest.

1. Copy and merge the `3ds` folder from the ctr-httpwn zip to **3DS #2's** SD card
2. Reinsert your SD card into **3DS #2**
3. Launch the homebrew launcher on the device using [Homebrew Launcher \(No Browser\)](#)
 - **Ensure menuhax is not installed, or you won't be able to return to Home Menu from the homebrew launcher**
4. Launch ctr-httpwn on **3DS #2**
5. Press (A) to continue
6. Press (Start) to exit ctr-httpwn
7. Press (Start) to open the homebrew launcher exit menu
8. Press (X) to Return to Home Menu (no reboot)
 - You may get an "Error has occurred" message with the option to continue. This is fine, just hit (A)
9. Continue to the next section **without rebooting**
 - **3DS #2** has been temporarily patched to allow network functions (such as System Transfer) without running the latest system version
 - Keep in mind that exiting the System Settings will reboot the system
 - If the system is rebooted, you'll have to re-run ctr-httpwn before System Transfer will work

Section V - System Transfer

1. **Backup every file on both 3DS's SD cards to two separate folders on your computer (keep track of which is which)!**
2. Reinsert each SD card back into their corresponding 3DS
3. If **3DS #2** has a Nintendo Network ID on it, you must format the device using System Settings:
 - Go to the last page of "Other Settings" and select "Format System Memory", then follow all instructions
4. Read the following:
 - Your CFW 3DS = 3DS #1 = "Source System"
 - Your Stock 3DS = 3DS #2 = "Target System"
 - **Move DSiWare titles if prompted!**
 - Do **NOT** delete the source system's SD card contents if prompted
 - Make sure neither device's battery dies during the transfer
5. Go to [this link](#) and follow Nintendo's official instructions for System Transferring from one system to another while keeping in mind what you just read

Section VI - Restoring 3DS #1

1. On **3DS #1**, complete initial setup
2. Do one of the following (*or neither if you don't mind 3DS #1's NNID being nonfunctional*)
 - Do the rest of the sections and then the full guide on **3DS #2**, then wait one week, then System Transfer from **3DS #2** back to **3DS #1** (*remember you cannot transfer back from a New 3DS to an Old 3DS*)
 - Go to the settings and attempt sign back into your initial NNID, then call Nintendo and ask about the error you get

3. Reboot **3DS #1** while holding Start to launch Hourglass9
4. Go to SysNAND Backup/Restore and restore SysNAND from `NANDmin.bin`

Section VII - Backing up 3DS #2's firmware

1. Copy `boot.nds` to the root of **3DS #2's** SD card
2. Create a folder named `dgTool` on the root of **3DS #2's** SD card if it does not already exist
3. Copy the contents of the firmware zip to the `dgTool` folder on the root of **3DS #2's** SD card
4. Launch your DSiWare game on **3DS #2**
5. Launch dgTool using your DSiWare game
 - Fieldrunners: Touch the 'Scores' button at the main menu
 - Legends of Exidia: After pressing (A) or (Start) at the two title screens, select the first save slot and press continue
 - Guitar Rock Tour: Scroll down and go to High-Scores -> Drums -> Easy
 - If your game does not have the hacked save file installed, [follow this troubleshooting guide](#)
6. Use dgTool to backup **3DS #2's** firmware
 - New 3DS: select "Dump F0F1_N3DS.bin"
 - Old 3DS or 2DS: select "Dump F0F1_O3DS.bin"
7. Make note of the firmware backup's location
8. Exit dgTool
9. Put your SD card in your computer, then copy `F0F1_N3DS.bin` or `F0F1_O3DS.bin` (depending on your device) to a safe location; make backups in multiple locations; this backup will save you from a brick if anything goes wrong

Section VIII - Flashing 3DS #2's firmware

1. Launch your DSiWare game on **3DS #2**
2. Launch dgTool using your DSiWare game
 - Fieldrunners: Touch the 'Scores' button at the main menu
 - Legends of Exidia: After pressing (A) or (Start) at the two title screens, select the first save slot and press continue
 - Guitar Rock Tour: Scroll down and go to High-Scores -> Drums -> Easy
3. Select "Downgrade FIRM to 10.4" and confirm to flash the 10.4.0 firmware bin to **3DS #2**
4. Exit dgTool
5. Reboot

Section IX - Exploit verification

1. Copy and merge the `3ds` folder from the 3DSident zip to **3DS #2's** SD card
2. Reinsert your SD card into **3DS #2**
3. Launch the homebrew launcher on **3DS #2** using [Homebrew Launcher \(No Browser\)](#)
4. Launch 3DSident
5. Verify that the following:
 - **Kernel version:** 2.50-11
 - **FIRM version:** 2.50-11
 - If either of these do not display the versions above, something has gone wrong and you should try again from the beginning

3DS #2's version number will *not* have changed in the settings.

Continue from [Homebrew Launcher \(No Browser\)](#), using steelhax for your entrypoint instead of one of the ones listed.

If, once transferred, steelhax only crashes to a black screen on **3DS #2**, [follow this troubleshooting guide](#).

For support, ask for help at [#3dshacks on Rizon IRC](#).

If you appreciate this guide, I accept [donations](#) through both Bitcoin and PayPal.

