

Forum:[Hack Forums](#)

Thread: [Exploiting the Playstation 3 | Everything you need to know!](#)

Bet - March 31, 2015, 3:38 am

[img]<http://www.castlevaniaspain.com/wp-content/uploads/2015/03/playstation-e3-banner.png>[/img]

[Nextgenupdate \(NGU\)](#)

[Trophies & Game Saves](#)

[Control Console API](#)

[PS3Lib](#)

[Manager API](#)

[Complete Software Collection \(SEX, DEX, CEX, OFW, CFW\)](#)

[Complete Homebrew Collection](#)

[Multi RPC](#)

[PS3Hax](#)

[Homebrew](#)

[Tutorials](#)

[Modding](#)

[Emulators](#)

[Console Crunch](#)

[Public CIDs](#)

[Protection from Stealers](#)

[Semi-Brick Fix](#)

[Downgrading/Upgrading Support](#)

[Portal Centric](#)

[Public CIDs](#)

[GTA V Modding](#)

[Call of Duty Modding](#)

[Battlefield Modding](#)

[IMG]http://##/jCpsbl.png[/IMG]

CEX= Consumer Version

Spoiler ([Click to View](#)) This simply means it is installed on the retail consoles that you bought at the store. It is what approx. 98% of consoles are.

DEX= Debug Version

Spoiler ([Click to View](#)) This is the version that is installed on debugging,/developer/testing PS3s that game/software developers get so they can make programs and patches for their products. It allows for Real Time Memory Editing and more debugging options like dual internet settings and HDD read speeds.

SEX= Shop Version

Spoiler ([Click to View](#)) This is the version that can be found in stores and is accompanied by kiosk/demonstration firmwares. It is what is found in the stores or shops.

OFW= Official Firmware / (DEX + CEX)

Spoiler ([Click to View](#)) This is the firmware that Sony releases and is what you update to when you connect through the internet to update. It has no debugging options and does not allow homebrew to run.

DFW= Demonstration Firmware / (SEX)

Spoiler ([Click to View](#)) This a firmware that you find on PS3s in stores that allow only for games/demos/videos to be run. It requires a 4 digit pin number to "unlock" the majority of its features but will never have all the settings unlocked for the user.

MFW= Modified Firmware(aka Kiosk Firmware) / (SEX + CEX)

Spoiler ([Click to View](#)) This firmware is a modified version to act like a retail firmware with debug options. All it adds is XMB options like "Install Package Files" but does not allow the install nor running of homebrew apps. It is utterly useless, do NOT install this on your PS3s.

CFW= Custom Firmware / (CEX + DEX)

Spoiler ([Click to View](#)) This is a modified retail firmware that does have debug options added to it and allows the installation plus the running of homebrew on the system.

PS3UPDAT.PUP

Spoiler ([Click to View](#)) The firmware file which you use to update your console.

Console ID

Spoiler ([Click to View](#)) The identity of your console, what sony often bans through.

PKG

Spoiler ([Click to View](#)) A package file, usually to install games, homebrew and software

NAND/NOR

Spoiler ([Click to View](#)) The PS3's Flash

Param.sfo

Spoiler ([Click to View](#)) A file which contains all the settings/preferences of games, contained in every single PS3 game.

SKU

Spoiler ([Click to View](#)) The stock-keeping unit

SDK

Spoiler ([Click to View](#)) This is the software-development kit, pretty self explanatory

XMB

Spoiler ([Click to View](#)) Xross media bar, the OS of the playstation 3

eBoot

Spoiler ([Click to View](#)) The file which is present in all PS3 games, containing various information and is vital to all CFW

[IMG]<http://#/NCONmo.png>[/IMG]

So, you've read the above and are interested in downgrading your PS3? Great! Well, you need to make sure your PS3 is downgradeable first.

Follow the below tables, you can find your Playstation model number [here](#).

Note: Super slims cannot be downgraded to 3.55 as they were released after this update was introduced.

PS3 FAT

Spoiler ([Click to View](#))

PS3 SLIM

Spoiler ([Click to View](#))

Hence, make sure your minimum firmware is not above 3.55, otherwise, you cannot downgrade or jailbreak.

[IMG]<http://#/nG7GSS.png>[/IMG]

So, you've checked your model number, and still want to go through with the downgrade? You will need to purchase a flasher, which will either be Progskeet, Teensy++ or the E3 Flasher (For Slims and some FATS).

Spoiler ([Click to View](#)) Fat PS3 with model numbers:

CECHA\CECHB\CECHC\CECHE\CECHG

Progskeet or Teensy++

Fat PS3 with model numbers:

CECHH\CECHJ\CECHK\CECHL\CECHM\CECHP\CECHQ
E3 Flasher

You can find cheap flashers on sites like [amazon](#), [ebay](#), or even [gumtree](#).

Remember, you will also have to either solder or use clips to attach the flasher to your PS3!

[IMG]http://#/oqKxNu.png[/IMG]

Congratulations, you have completed the hard part of this tutorial! You now simply need to install CFW. I recommend Rogero 4.50 (CEX) for noobies and people who have less to moderate experience with this stuff.

You can find a full link to all CFW/OFW below.

Spoiler ([Click to View](#))

<http://www.nextgenupdate.com/forums/ps3-cheats-customization/658052-complete-ofw-cfw-dex-sex-mfw-ps3-collection.html>

All you need to do is get a USB Flash Drive (Formatted in FAT32). Make these folders, in this order, all in capitals.

PS3 > UPDATE > PS3UPDAT.PUP

Then, just to go on your PS3, hit system update and via storage media and select your update via USB.

[IMG]http://#/6YMJ3T.png[/IMG]

[Multiman](#)

This is pretty much essential for your PS3, it will allow you to FTP to and from your PS3, run games from your internal/external HDD, and provide you with a file manager!

[PSN Patch](#)

This will allow you to spoof your console's settings into letting you play online in future updates as well as make your PS3 more safe to go online!

[CCAPI](#)

This Homebrew is really useful for modding since it will allow you to change your console ID in case you ever get the system banned, It also allows you to edit the offsets in a game. For example: 0x001bbbc2c. Editing that offset will change your name in Modern Warfare 3.

[PS Jailbreak Manager](#)

PS JBM is extremely useful and is essential to all individuals with CFW. You can easily customise, edit all types of things with this manager, including menus, backgrounds, games etc.

[Comgenies Awesome Filemanager](#)

This is a file manager is subjectively the best file manager available to PS3 users. It has very sleek GUI, which maximises your managing experience. You can edit files, transfer to and from the FTP using this homebrew.

[PKGView](#)

This basically enables you to view all PKG files through your PS3 system/file managers.

[Resigning Tools](#)

Assists in the process of resigning game saves, extremely useful if you are interested in modding single player games.

[IMG]<http://M1LKvV.png>[/IMG]

You're bored of your boring jailbroken console, and want to get even deeper into it? Extreme caution is advised, you risk the possibility of completely destroying your console!

[Video: https://www.youtube.com/watch?v=uxzxBFf63_8]

Downloads:

[IDPSet v0.84](#)

CEX to DEX (Without Flash Dumps)

Spoiler ([Click to View](#))

1. Download & Install the .pkg file on your PS3.
2. Open Rebug Toolbox.
3. Make sure Toggle QA Flag is Enabled.
4. Restart the PS3.
5. Run the IDPSet.
6. Select "Dump eid_root_key". When finished you will be returned back to the menu.
7. Select "Make CEX & DEX Dumps". When finished you will be returned back to the menu.
8. Select "Convert to DEX". When finished your system will be restarted.
9. Open Rebug Toolbox.
10. Select "System Information".
11. If it says "LV2 Kernel: DEX", "Target Type: DEX", you have successfully converted to DEX.

DEX to CEX (Without Flash Dumps)

Spoiler ([Click to View](#))

1. Download & Install the .pkg file on your PS3.
2. Open Rebug Toolbox
3. Make sure Toggle QA Flag is Enabled.
4. Swap LV2 Kernel.
5. Restart the PS3.
6. Run the IDPSet.
7. Select "Dump eid_root_key". When finished you will be returned back to the menu.
8. Select "Make CEX & DEX Dumps". When finished you will be returned back to the menu.
9. Select "Convert to CEX". When finished your system will be restarted.
10. Open Rebug Toolbox.
11. Select "System Information".
12. If it says "LV2 Kernel: CEX", "Target Type: CEX", you have successfully converted to CEX.

CEX to DEX (With Flash Dumps)

Spoiler ([Click to View](#))

1. Open Rebug Toolbox.
2. Rewrite Target ID in Flash.
3. Swap LV2 Kernels.

DEX to CEX (With Flash Dumps)

Spoiler ([Click to View](#))

1. Open Rebug Toolbox.
2. Rewrite Target ID in Flash (It will automatically swap kernels).

Experiencing issues while dumping eid_root_key?

Spoiler ([Click to View](#))[eid_root_key Dumper 4.70](#)

1. Download & Install the .pkg file(s) on your PS3.
2. Open Rebug Toolbox
3. Make sure Toggle QA Flag is Enabled.
4. If on DEX, Swap LV2 Kernel.
5. Restart the PS3.
6. Run EID Root Key Dumper. It will restart your PS3.
7. Run IDPSet.
8. Select "Make CEX & DEX Dumps". When finished you will be returned back to the menu.
9. Select "Convert to CEX" or "Convert to DEX". When finished your system will be restarted.
10. Open Rebug Toolbox.
11. Select "System Information".
12. If it says "LV2 Kernel: CEX", "Target Type: CEX", you have successfully converted to CEX.
- 12(b) If it says "LV2 Kernel: DEX", "Target Type: DEX", you have successfully converted to DEX.

[IMG]<http://CariXS.png>[/IMG]

Avoiding Bans

Download: [PS Ninja](#)

- Appear offline (using PS Ninja)
- Never, never open any homebrew while signed into PSN
- Often wipe and replace history using PS Ninja
- Always change your CID to a random string of numbers or letters after signing in (spoofing your CID will prevent sony from seeing it)

Unbanning Yourself

The only way to unban yourself is by using homebrew (such as CCAP) in order to change your Console ID. You must have a valid Console ID.

NOTE: You can not unban a PSN account, once it's banned for modding, it's gone for good.

Protection from CID Stealers

What we will be doing is simply blocking the internet connection of the tool, so any data cannot be sent anywhere except to and from your own PS3.

1. Open 'Windows Firewall with Advanced Security'
2. Click on Outbound Rules
3. Click on new rule, ensure the only thing that is checked is program, and click next
4. Leave all other options, and select the tool you want to block the connections of
5. Make sure you only click 'Block Connection' in the window that pops up
6. Click next, and name the rule whatever you would like

Changing a discs region (BLES/BLUS etc.)

Always remember to keep back ups of previous files, in case of corruption/errors

Using a file manager, navigate to the game folder you want to convert (usually /dev_hdd0/GAMES
Open the game folder BLXXXXXX and locate PS3_DISC.SFB. Open the SFB file and change the
game id to whatever BLES/BLUS you want.

Navigate to the file location /BLXXXXXX/PS3_GAME/, locate the PARAM.SFO, and once again
change it to the BLES/BLUS desired.

Navigate to the file location /BLXXXXXX/PS3_GAME/LICDIR, Open the LIC.DAT file and change
the BLES/BLUS in there.

Finally, rename all the game folders to whichever game ID you have set to, it should now be fine
and ready to use.

Nice Net Bro - March 31, 2015, 3:40 am

Nice thread this will help the noobs out ?

Billie Joe - March 31, 2015, 3:43 am

Nice tutorial Tick. Good shit bro. ?

?Young Thug - March 31, 2015, 3:45 am

Nice tutorial. My PS3 Blew Up What do i do now?

?homas - March 31, 2015, 4:08 am

Damn, HQ thread man! Vouch for this nice person OBVIOUSLY knows what he is talking about.
(PS, Give me more credits on VG)

Bet - March 31, 2015, 7:33 am

Thanks guys, if you have anything you'd like me to add, feel free to suggest! ?

Tenno - March 31, 2015, 8:34 am

You could add that if you're modding on DEX, you do not need to use offsets on CCAPI. You can
just download an RTM tool that has the namechange option.

EDIT- You should also add that superslim's cannot be downgraded.

Bet - March 31, 2015, 8:38 am

(Mar 31, 2015 08:34 AM)Tenno Wrote: [\[CITE\]](#) You could add that if you're modding on DEX, you do
not need to use offsets on CCAPI. You can just download an RTM tool that has the namechange
option.

EDIT- You should also add that superslim's cannot be downgraded.
Superslim part was already there, but I'll add the dex/ccapi part soon.

Tenno - March 31, 2015, 8:44 am

(Mar 31, 2015 08:38 AM)Tick Wrote: [\[CITE\]](#) Superslim part was already there, but I'll add the
dex/ccapi part soon.Oh, didn't see that :) Great tutorial though, would you mind if I added your post
to my jailbreaking help desk? I will leave proper credit.

Check it out: <https://hackforums.net/showthread.php?tid=4755059&pid=45481073#pid45481073>

Bet - March 31, 2015, 8:47 am

(Mar 31, 2015 08:44 AM)Tenno Wrote: [\[CITE\]](#) Oh, didn't see that :) Great tutorial though, would you mind if I added your post to my jailbreaking help desk? I will leave proper credit.

Check it out: <https://hackforums.net/showthread.php?tid=4755059&pid=45481073#pid45481073>
Of course, feel free ?

Apostle - March 31, 2015, 9:26 am

Nice thread man, going for that sticky? ;)

RatchetB?ooty - March 31, 2015, 12:01 pm

Nice informative HQ thread Tick! Good job. This should help the people who have just got a CFW on there PS3 ?

Telstra - March 31, 2015, 4:48 pm

Wow, I didn't know you knew this sort of stuff Tick. Very interesting read, and quite informative.

Doodlebob™ - March 31, 2015, 4:51 pm

Instructions not clear enough, dick stuck in my flasher.

/jokes

Great thread, will surely help newbies out. I recommend adding the fact that you can get downgrade services for a lot cheaper than flashers themselves and it'll be much easier, that's what I've been doing in the past. PS3Hax has a lot of downgrade services.

MeIT3d - March 31, 2015, 6:58 pm

Looks like a lot of work went into this. Looks wonderful!

The Judge - March 31, 2015, 7:51 pm

Amazing guide tick, this definitely deserves a sticky.

Cyrus - March 31, 2015, 11:05 pm

I have an old CFW in the cupboard that is on DEX, I don't fucks with Consoles nomore it just stays in the cupboar I cba with needing to get hold of CID's all the time because mine is banned lol.
Plus I don't fuck with consoles at all anymore.

I wish MW2 never died out well wish the servers on MW2 PS3 never died out.
I remember the first lobbies with DEREKTROTTER etc, I use to be in partys with him and a few others sometimes back when it all began lol

Tenno - April 1, 2015, 1:55 am

(Mar 31, 2015 11:05 PM)Cyrus Wrote: [\[CITE\]](#) I have an old CFW in the cupboard that is on DEX, I don't fucks with Consoles nomore it just stays in the cupboar I cba with needing to get hold of CID's all the time because mine is banned lol.
Plus I don't fuck with consoles at all anymore.

I wish MW2 never died out well wish the servers on MW2 PS3 never died out.
I remember the first lobbies with DEREKTROTTER etc, I use to be in partys with him and a few others sometimes back when it all began lol I remember the old days with Elitemossy and people modding the fuck out of online matches. Too bad patch_ff.mp is patched. Now there's only kids asking for CFG infections and copy/pasting CFG codes.

I remember I tried to get RedDotCity's menu when I was on 3.55. Right before I was going to

jailbreak, a new update came out and I was like "okay, I'll update" but of course, the 3.56 update patched jailbreaking via XMB :/

TheyCallMeFox - April 1, 2015, 5:17 am

Wow. Real HQ Thread for people who are starting.

Bet - April 2, 2015, 12:07 am

Glad to see this thread is helping people ?

Income. - April 2, 2015, 11:06 am

Very informative thread it's covering up a lot of good things to know. I'm sure this will be useful for some beginners.

Bet - April 3, 2015, 4:10 am

Thanks for the kudos for the thread. I hope it does indeed help people!

Bet - April 3, 2015, 4:11 am

Thanks for the kudos for the thread. I hope it does indeed help people!

QuantumHD - April 3, 2015, 4:59 pm

Heyy, do you know any good sites where i can download good working eboots? Im on 4.50 Rogero cex.

Bet - April 3, 2015, 7:58 pm

(Apr 3, 2015 04:59 PM)QuantumHD Wrote: [\[CITE\]](#) Heyy, do you know any good sites where i can download good working eboots? Im on 4.50 Rogero cex.

I would suggest you get them from one of the game modding site under your game's corresponding section.

Nas - April 4, 2015, 9:01 am

Pretty decent thread. It covers most of the things you need to know.

Bet - April 5, 2015, 11:15 pm

(Apr 4, 2015 09:01 AM)-Nas Wrote: [\[CITE\]](#) Pretty decent thread. It covers most of the things you need to know.

Thanks Nas! Appreciate it! Hopefully more people see this thread instead of making threads on basic questions ?

Maximum - April 8, 2015, 8:21 pm

Great tutorial Tick, I'm sure it'll help a ton of people out.

Bet - May 25, 2015, 8:14 pm

Thanks, going to this up for anyones questions.

Funtage - May 25, 2015, 8:14 pm

how has this not been stickied!!!

QuantumHD - May 26, 2015, 2:40 pm

Nice tutorial man! Great for new modders.

nondescriptoldie - May 27, 2015, 9:04 am

Brilliant thread man! :P

Explains in detail all the core things you need to know and have!

Well done, no surprise from a HQ user like you though!

Bet - September 9, 2015, 7:16 pm

Thought I'd bring this to the top to help some people out

Gustav - September 13, 2015, 6:15 am

Huge vouch for tick, insane tutorial right here.

SIM-2434055 - September 13, 2015, 7:33 am

Nice tutorial even though I don't own one.

?

Bet - September 13, 2015, 9:35 am

Thanks for the feedback guys, OP is updated so it contains much more info!

DOSH - September 13, 2015, 10:22 am

You should also use psnpatch to avoid a ban.

Maximum - September 13, 2015, 1:52 pm

Nice tutorial with a lot of helpful information.

SIM-888979 - September 13, 2015, 6:41 pm

wtf is this dumb shit i just wanna play cod?

Tenno - September 13, 2015, 11:12 pm

You should also add Infectus as a flasher if you have a NAND chip (phat)

WuTangClan - September 14, 2015, 11:47 am

(Sep 13, 2015 10:22 AM)Force?? Wrote: [\[CITE\]](#) You should also use psnpatch to avoid a ban. PSNPatch is outdated. Just use ccapi for OFW.

Bet - August 18, 2016, 12:55 am

Keeping this relevant .

dongle - December 25, 2016, 1:17 am

You should mention some things about spoofing for the noobs.

To get online, use the following homebrews to accomplish the desired tasks:

- 1) SENEnabler - Spoof to latest firmware
- 2) PSNinja - Clear history etc
- 3) PSNPatch - Disable cfw

Tree of Life - December 25, 2016, 1:57 am

(Dec 25, 2016 02:17 AM)dongle Wrote: [\[CITE\]](#) You should mention some things about spoofing for the noobs.

To get online, use the following homebrews to accomplish the desired tasks:

- 1) SENEnabler - Spoof to latest firmware
- 2) PSNinja - Clear history etc
- 3) PSNPatch - Disable cfw

I don't use any of that shit and I've had my console ID for over a year. In fact, when I did use these, I was banned. Soo I don't know.. maybe it's just me but these homebrew apps don't seem to useful.

Zach_Farlow - *December 25, 2016, 2:13 am*

nice thread man i could really use it