Откат прошивки 3.60 и 3.70 для PS3 Slim

Послан magicdevice - 19.08.2011 17:15

Downgrade For Slim PS3 Slim Consoles On Firmware 3.70

у нас есть возможность сделать даунгрейд для PS3 Slim. На этот раз даунгрейд был сделан немного по-другому, в отличии от PS3 FAT, я сделал его с помощью 2 чипов, progskeet и teensy++ (достаточно любого из этих чипов).

Для начала даунгрейда вам необходимо:

1) PS3 FAT или Slim с установленной прошивкой 3,70 (Не пытайтесь сделать тоже самое с другой версией прошивки).
2) Чип для чтения и записи PS3 NOR Flash (чип progskeet или teensy+ +).
3) HEX редактор (рекомендую использовать hxd).
4) FlowRebuilder v.4.1.3.2.
5) Холодное пиво (самый важный компонент).
6) Downgrade.bin (ссылка на скачивание в конце новости).

Сначала сделайте дамп NOR Flash размер которого, должен быть "16777216 байт", ни одним байтом больше, ни одним байта меньше и вы должны быть абсолютно уверенно в том, что вы делаете, и у вас должен получиться дамп, например "jakemcallister.bin". Откройте его с помощью программы flowrebuilder. Чтобы сделать этот файл доступным для чтения выберите опцию, которая называется bytereverse dump и затем выберите extract.

После того, как вы это сделаете, у вас должен появиться файл, но с расширением bin.REV. Откройте его в программе HxD и скопируйте из него ваши личные данные консоли: EID, BOOTLOADER, CSID и METLDR.

Больше данных оттуда нам не нужно.

Дальше вы берете наш METLDR из нашего prepatched image из нашей папки даунгрейда, в которой flowrebuilder поместил our.rev также создал другую папку под названием "nameofthedump.EXT" в нем находятся наша персональная информация о консоли и вы должны её немного изменить в нашем prepatched image.

Откройте программу HxD и с помощью нее откройте файлы downgrade.bin и metldr, которые находятся внутри папки asecure_loader. В программе HxD выбираем вкладку metldr и копируем в нее все содержимое HEX файла downgrade.bin.

Дальше в программе нажмите control + g и напишите в появившимся окне "810". Это и будет позицией metldr и нажмите правой кнопкой мыши на первой строке в позиции 810.

Выберите функцию «вставить с заменой" и таким же образом сделайте с остальными файлами:

METLDR : offset “810″ size “E960″
BOOTLOADER_0 Offset“FC0000″ size “40000″
EID: Offset “2F000″ size “10000″
CISD: Offset“3F000″ size “800″

Теперь берем файл downgrade.bin с сохраненными изменениями, и запускаем программу

flowrebuilder и выбираем функцию bytereverse dump и затем extract.
На этот раз программа выдаст нам ошибку, но все так и должно быть и после этого, программа создаст нам файл с названием downgrade.bin.REV.

И этот файл, который вы должны внести во flash консоли.

Если вы все сделали правильно, то при включении консоли, и вы увидите на экране надпись, нажмите кнопку PS. НИЧЕГО НЕ НАЖИМАЙТЕ, выключите консоль и введите её в factory service mode. Как только вы это сделаете, вы должны сделать правильную файловую систему с помощью 3,55 lv2diag от jaicrab без чтения информации и с помощью специального CFW. (ссылки на них в конце новости)
Затем включите консоль с флешкой с этими двумя файлами в правом порту USB (обязательно именно в правом), и консоль автоматически выключится через 10/15 минут. Затем включите консоль без всяких USB устройств подключенных к ней и, если вы все сделали правильно, вы зайдете в XMB.

Если вы вошли в XMB, то выключите консоль и на флешку скопируйте файл из архива Lv2diag_355.rar.

Консоль будет включена на 20 секунд и затем автоматически выключится, и ПОЗДРАВЛЯЕМ теперь у вас консоль с прошивкой kmeaw CFW 3,55.

==========