[MAJ 2] Downgrader une v3.70 en v3.55

Soumis par Hamato
17-08-2011

Rappel : Mardi 16 Août 2011, une team Italienne, DiGiTaL AnGeL, a annoncé avoir réussi à downgrader une PS3 possédant un firmware 3.70 vers le firmware 3.55. Par ici notre annonce .

Aujourd'hi, Mercredi 17 Août 2011, nous vous relayons, la méthode.

Cette méthode de downgrade, qu'on peut appeler Tuto, a été distribuée par dospiedras1973, un membre du site espagnol Elotrodao.

En attendant qu'un MétaGamer puisse tester par lui-même, et donner un retour, la manipulation traduite en français (enfin du mieux que je pourrai) sera accessble dans la suite de ce billet, et relayée sur le forum.

Pour venir en discuter avec nous, sur le forum c'est par ce lien que ça se passe.

Source : Elotrolado

[TUTO RELAYE EN FRANCAIS]

Avant de commencer :

DISCLAIMER :

Ceci n'est pas un tuto fait par MétaGames mais juste une traduction française de l'original : toute correction est la bienvenu. Attention ni moi, ni MétaGames, ni les Développeurs des logiciels/fichiers ... ne pourrons être tenu responsables en cas de problème avec votre console ! Blablabla ...

[MISE A JOUR 2] :

ps3hax.net a fait un tuto en anglais clair (avec posage de la progskeet par exemple) : ICI

[MISE A JOUR] :

Dospiedras1973 a créé une automatisation de l'édition Hexa (tant mieux je n'étais pas sûr de ces étapes ^^)

Télécharger l'outils.

Il faut mettre bytereversed en "émetteur/donneur" et downgrade.bin en "récepteur".

Ainsi les étapes 3-4-5-6 sont simplifiées et ne correspondent plus exactement à ce qui est écrit par la suite.

Si à un moment, l'écran devient rouge (RSOD), il faut arrêter tout de suite, et il sortira un downgrade v2 qui aura fixé le problème.

Il nous faut :

- Une console PS3 Slim ou FAT, avec une Nor mise à jour en 3.70 : Ne pas essayer avec une autre version !
- De quoi écrire dans la Nor : un Tensy++ ou une puce progskeet
- Le logiciel hxd (c'est un éditeur héxadécimal, il se trouve qu'il y a un raccourci clavier utilisé, donc si vous avez le même ça sera top, sinon il faudra trouver vous-même la correspondance)
- FlowRebuilder v 4.3.1.2 (c'est un logiciel qui permet d'extraire du contenu de nos dumps)
- Une bière fraiche (Ce point est important) XD Perso je conseille rien du tout, imaginez qu'une goutte tombe dans la console : bwahahaha. Ou alors si c'est pour anesthésier le cerveau, cognez vous la tête ^^
- Le Downgrade.bin : ICI

Ce qu'on doit faire :

- En premier lieu : Dumper la Nor avec le flasher utilisé

- Vérifier que l'archive obtenue fait exactement 16 777 216 bytes (= 16 777 216 octets). Ni plus, ni moins. Pour être sûr de vous, faites plusieurs dumps. Bon ok ça serait pas de chance que sur 50 dumps, ça soit tout le temps des mauvais ^^

- Normalement un beau petit .bin doit être créé

- Ouvrir ce fichier avec FlowRebuilder, pour avoir une archive utilisable. Choisir l'option bytereverse and extract nor dump

- Cette fois on doit avoir un fichier .bin.rev

- Ouvrir avec hxd, et récupérer les données persos de la console : EID, BOOTLOADER, CSID et METLDR. Procédé de l'extraction : (ici l'exemple pour le METLDR) :

- FlowRebuilder a créé le .rev. Dans le même dossier se trouve un autre dossier (Attention c'est INCEPTION ^^) Dans ce nouveau dossier un fichier "NomDuDump.EXT"

- Ouvrir l'éditeur Héxa (c'est hxd) pour afficher le fichier downgrade.bin, et le fichier METLDR contenu dans le dossuer asecure_loader

- Choisir l'onglet METLDR, et copier le contenu entier. Choisir ensuite l'onglet downgrade.bin

- Faire control + g, et écrire 810

- Faire un clic droit sur la première ligne de la position 810 et choisir de coller les données

- Voici les données à copier dans le downgrade.bin

- METLDR : position 810, et taille E690

- BOOTLOADER_0 : position FC0000 et taille 40000

- EID : position 2F000 et taille 10000

- CISD : position 3F000 et taille 800

- Une fois terminé, enregistrer le tout et ouvrir le downgrade.bin dans FlowRebuilder

- Choisir l'option bytereverse. Normalement on vous gueule dessus parce qu'il y a une erreur : c'est normal

- Un fichier downgrade.bin.rev a du être créé : c'est lui qu'on va utiliser pour flasher la console. Là faut flasher la console :P

- Si tout c'est bien déroulé, allumer la console. Normalement on nous demande d'appuyer sur le bouton PS : Ne pas appuyer sur ce bouton ! Eteindre la console : interrupteur ou alors débrancher.

- Se mettre en mode "Factory" (mode usine, j'ai oublié le nom qu'on donne en Français ^^)

- Quand c'est fait il faut récupérer le Lv2diag.elf (patché par Jaicrab) disponible sur LS apparemment : http://www.logic-sunrise.com/telechargement-225750-lv2diag-patche-par-jaicrab.html

- Récuperer ce CFW : http://pastebin.com/03MFDLGV

- Mettre ces 2 fichiers sur une clé USB. La brancher sur le port USB de droite (= le port n°2), allumer et laisser faire. Ca s'éteindra tout seul au bout de 10/15 minutes

- Débrancher la clé et rallumer. Normalement on doit revenir sur le XMB

- Si c'est ok. On éteint (encore lol), on vide la clé usb et on met ce Lv2diag : http://pastebin.com/gGETcxMR

- On rallumes, la console restera environ 20 secondes allumée et s'éteindra d'elle même.

- GG, votre console est 100% fonctionnelle et tourne sous le 3.55 Kmeaw

REMERCIEMENTS A (je laisse en espagnol vous comprendrez par vous même)

- DiGiTaLAnGeL (Tester con progskeet)

- Glevand & mfw builder team(cfw)

- NDT (Ayudante) Es muy buena persona

- JaiCraB (lv2diag sin lector)

- Robs1 (mi guia con las nor flash)

- EussNL (su gran apoyo en la wiki que utilizo todos los dias PS3DEVWIKI.COM)

- Defyboy (por crear ps3devwiki)

- A todo el canal #darkps3 de irc-hispano.org por sus apoyos y tantas horas de pruebas que nos hemos pegado eh cabrones!!!

- DemonHades (gracias a que si no hubieras puesto la portada en tu web con la mentira que contastes sobre mí, no hubiera conocido a DigitalAngel ni a uf6667 y estos dos me han ayudado mucho)

-

- y por ultimo la gente me ha pedido por privado que ponga un boton de paypal para donar , pues aqui lo teneis :

- https://www.paypal.com/cgi-bin/webscr?c ... 5EYNQJ6H62

-

- saludos y apartir de ahora reanudaré mi trabajo con la dual nand y ese dump de 3.6x que tantos problemas me da jejej

-

- por cierto aprovecho para poner que os aconsejo que no lleveis vuestra consola a una tienda llamada chipdress , ya van dos personas se han puesto en contacto conmigo para reparar el destrozo que hicieron en sus consolas los de dicha tienda , BEWARE

-