PSP - Geschichte der Custom Firmwares

Thorsten ’Atsutane’ Toepper

10. September 2009

Übersicht

Vorstellung der PSP Modelle

Begriffserläuterung

Historie der Sony Firmwares

Exploits

Werdegang der Custom Firmwares

Pandora’s Battery - Die JigKick Battery und der Magic Memory Stick

Sonstiges und Quellen

Vorstellung der PSP Modelle

PSP 1000 / FAT

- Erschien im September 2005 in Europa
- 480x272 Auflösung, 4,3 Zoll Display
- 32Bit MIPS CPU (333 MHz)
- 32MB RAM

PSP 2000 / Slim&Lite

- Erschien im September 2007 in Europa
- Gewicht um 33% verringert
- etwa 20% dünner
- 64MB RAM
- TV-Ausgang
- UMD-Cache

PSP 3000 / Slim&Lite

- Erschien im Oktober 2008 in Europa
- „Verbessertes“ Display
- Weitere Schutzmaßnahmen gegen das aufspielen alternativer Firmware

Begriffserläuterung

Begriffserläuterung

Homebrew
Nicht signierte Software von Hobbyentwicklern.

Homebrewenabler - HEN
Exploits um Homebrews zu starten.

IPL
Initial Program Loader

XMB
Cross Menu Bar - Das Menü der Firmware

Historie der Sony Firmwares

1.xx Kernel

1.00 - 12 Dec 2004

- Keine Code Authorisierung
- Nur auf den ersten japanischen Modellen

1.50 - 24 Mar 2005

- Code Authorisierung
- Mehrsprachig

1.51 - 18 May 2005

- KXploit gefixt
- Mehrsprachig

1.52 - 15 Jun 2005

- Weitere Patches

2.xx Kernel

2.00 - 1 Sep 2005 *

- u.a. Browser, WPA, MP4 und WAV Support, verschiedene Bildformate und Wallpaperfunktion hinzugefügt

2.01 - 3 Oct 2005

- TIFF-Exploit gefixt

2.50 - 13 Oct 2005 *

- Browser verbessert
- WPA-PSK(AES) Support hinzugefügt
- DRM geschützte Videos können abgespielt werden

2.60 - 29 Nov 2005

- Audio Podcast Support im RSS Reader

2.70 - 25 Apr 2006

- Adobe Flash Player hinzugefügt

2.71 - 30 May 2006

- Demos können über den Browser geladen und installiert werden.

2.80 - 27 Jul 2006 *

- Video Podcast Support im RSS Reader
- Im geheimen sceKernelLoadExec gefixt, netterweise sceRegOpenRegistry geöffnet.

2.81 - 7 Sep 2006

- Support für Memory Sticks größer als 4GB
- libtiff Exploit gefixt

2.82 - 26 Oct 2006

- Diverse Sicherheitspatches

3.00 - 21 Nov 2006

- Playstation 3 Remote Play
- PSOne Emulator - Fullspeed(!)
- Musikvisualisierung

3.01 - 22 Nov 2006 & 3.02 - 6 Dec 2006

- Playstation Network Titelunterstützung verbessert/erweitert

3.03 - 20 Dec 2006

- Playstation Network Titelunterstützung verbessert/erweitert
- Unterstützung der PSPCam

3.10 - 30 Jan 2007 *

- Dynamischer Normalizer
- Möglichkeit zum reservieren von Speicher hinzugefügt
- Im Geheimen Reparatur des sceRegOpenRegistry und des GTA Exploits

3.11 - 8 Feb 2007 *

- Playstation Network Titel können resettet werden

3.30 - 28 Mar 2007 *

- Thumbnail Support im RSS Reader
- MP4/H264 unterstützen nun auch weitere Äuflösungen: 352x480, 480x272, 720x480
- Wireless Hotspot Funktion hinzugefügt.

3.40 - 20 Apr 2007

- Playstation Network Titelunterstützung verbessert/erweitert.
- Zertifikats Option entfernt
- Savegames des PSOne Emulators mit denen des Emulators der PS3 kompatibel gemacht.

3.50 - 31 May 2007

- Remote Play via Internet möglich
- RSS Channel Guide hinzugefügt.
- CPU Limit entfernt, möglich mit 333MHz statt 266MHz zu nutzen.

3.51 - 29 Jun 2007

- Illuminati Exploit gefixt

3.52 - 24 Jul 2007

- Playstation Network Titelunterstützung verbessert/erweitert.

3.60 - 10 Sep 2007

- Erste Slim Firmware, führte Slim Features ein.

3.70 - 11 Sep 2007 *

- Erste Universelle Firmware (Für 1000 und 2000)
- Custom Themes
- Video: 2Mbit/s Bitratengrenze(vorher 768Kbit/s), Szenensuche, Sequenzielles Playback
- Musik hören während des betrachtens von Fotos möglich

3.71 - 13 Sep 2007

- Mal wieder einiges an Verbesserungen der „Sicherheit“
- Playstation Network Titelunterstützung verbessert/erweitert.
- Einstellungen für manche Regionen korrigiert.

3.72 - 30 Oct 2007

- Playstation Network Titelunterstützung verbessert/erweitert.
- Remote Start hinzugefügt(benötigt PS3)

3.73 - 29 Nov 2007

- Systemstabilität wiederhergestellt, einige Probleme mit dem UMD Laufwerk behoben.

3.80 - 17 Dec 2007 *

- OPML Support für den RSS Reader
- Player für Audio Streams hinzugefügt

3.90 - 29 Jan 2008 *

- Go! Messenger hinzugefügt.
- Slim: Skype hinzugefügt(außer in Japan).

3.93 - 18 Mar 2008 *

- Playstation Network Titelunterstützung verbessert/erweitert.
- Slim: Skype auch in Japan hinzugefügt.

3.95 - 8 Apr 2008

- Playstation Network Titelunterstützung verbessert/erweitert.
- PSOne Emulator: Belegung der Buttons konfigurierbar.
- Remote Play verbessert.

3.96 - 4 Jun 2008

- Nur mit Hot Shots Golf 2 auf UMD veröffentlicht.
- Playstation Network Titelunterstützung verbessert/erweitert.
- Einige Bugs gefixt.

4.00 - 18 Jun 2008

- Google Suche ins Menü integriert.
- Abspielgeschwindigkeit von Videos anpassbar.
- Untertitel Support für UMD Filme.

4.01 - 25 Jun 2008

- Darstellung der Suchergebnisse für manche Sprachen verbessert.
- Verbesserung der Wiedergabe einiger Videoformate.

4.05 - 13 Jul 2008 *

- Slim: In Japan ist die Aufnahme von TV Programmen möglich.

4.20 - 14 Oct 2008

- Erste Firmware für das 3000er Modell.
- Einführung der PSP 3000 Features.

4.21 - 14 Oct 2008

- Behebung eines Bugs in der libtiff.

5.00 - 15 Oct 2008 *

- Erste universelle Firmware für alle bisherigen Modelle.
- PlayStation Network als XMB Kategorie hinzugefügt.
- PlayStation Store dem Netzwerkmenü hinzugefügt.
- Timer dem Musikplayer hinzugefügt.
- USB Auto-Connect den PSP Modellen 1000 und 2000 hinzugefügt.
- Neue Vollbild Bildschirmtastatur hinzugefügt.
- MPEG-4 AVC (H.264) mit 640x480 Pixeln wird als Videoformat unterstützt.
- Screen capture in Spielen/Browser hinzugefügt.(Hängt von Spiel/Webseite ab)
- 3000: Vollbild TV-Ausgabe von PSX Titeln.

5.01 - 22 Oct 2008

- Bugfix: 8GB und 16GB Memory Sticks wurden bei Downloads aus dem Playstation Store, auch bei genügend Platz als voll erklärt.

5.02 - 20 Nov 2008 *

- Stabilität von Systemsoftware(u.a. Playstation Store) verbessert.

5.03 - 20 Jan 2009

- Stabilität von Systemsoftware(u.a. Playstation Store) verbessert.
- Gripshift Exploit gefixt.

5.05 - 19 Feb 2009

- Kompatibilitätsupdate für einige Spiele.

5.50 - 21 Apr 2009

- Information Board Board hinzugefügt.
- Verbesserungen im Memory Stick Stack(Unterordner für Videos und Fotos, Downloads aus dem Store brauchen weniger Platz).
- Internet Suche für Spiele direkt ins XMB integriert.
- Trend Micro Demo wurde in den Browser integriert.
- Exploit der libTIFF gefixt.

5.51 - 11 Jun 2009

- Systemsoftware stabilisiert.
- Kernel Exploit, welcher von ChickHEN verwendet wird, gefixt.

5.55 - 6 Jul 2009

- Kommt nur mit einigen Spielen.
- Nur für diese Spiele benötigt.

Exploits

Typen

Downgrader
Exploits welche das aufspielen älterer Firmwares ermöglichen, nur für die PSP 1000 interessant, da es so möglich war die Firmware 1.50 zu verwenden.

Homebrewenabler
Exploits, welche das starten von Homebrewapplikationen auf verschiedenen Sony Firmwares ermöglichen, vor allem für die späteren PSP 2000 Modelle und das PSP 3000 Modell von Relevanz.

Homebrew
Exploits welche das starten von nicht signiertem Code ermöglichen.

Pandora’s Battery
Hat ein eigenes Kapitel nach den Custom Firmwares.

1.50 Downgrader auf 1.0

Aufgrund der Homebrewinkompatibilität zu 1.50er Homebrew nicht interessant.

2.00 Downgrader

Der erste Downgrader für die Firmware 2.00 wurde von Fanjita entwickelt und setzte über einen Bug in der libtiff die Firmware Version auf 1.00, so dass die PSP das Update auf 1.50 annahm, da sie glaubte es sei ein Update.

2.01 Downgrader

Selbe Funktionsweise wie der Downgrader für 2.00 allerdings über eine andere Lücke in der libtiff, da die im anderen Exploit verwendete mit dieser Firmware geschlossen wurde.

2.50/2.60 Downgrader

Funktionsweise nicht bekannt. Funktionierte allerdings nicht auf Modellen mit den TA-082 und TA-086(Brick).

2.71 Downgrader - 1 Sep 2006 (FW 30 May 2006)

Von Dark Alex veröffentlicht, abermals über einen Bug in der libtiff. Nach wie vor für TA-082 Boards unmöglich.

2.71 Downgrader TA-082 - 27 Dec 2006 (FW 30 May 2006)

Von Dark Alex, harleyg und Mathieulh veröffentlicht, machte das installieren von FW 1.50 auf TA-082 PSPs welche mit 2.71 ausgeliefert wurden möglich, dies war zuvor durch Inkompatibilität einiger IDStorage Keys nicht möglich, diese wurden nun ausgetauscht und erst dann der eigentliche Vorgang ausgeführt.

2.80 Downgrader - (FW 27 Jul 2006)

- 23 Dec 2006: Von 0okm veröffentlicht.
- 24 Dec 2006: csfreakno1 veröffentlicht eine Benutzerfreundlichere Variante von 0okms Exploit.
- 2 Jan 2007: 0okm veröffentlicht einen 2.80 auf 2.71 Downgrader für TA-082/TA-086 PSPs, um diese im Anschluss mit Dark Alex Downgrader auf FW 1.50 zu bringen.
- Später veröffentlichte Team NOOBZ(u.a. Fanjita) einen sichereren Downgrader, welcher auf Dark Alex HEN basierte und direkt auf Version 1.50 downgradete, indem direkt überprüft wurde ob es sich um ein TA-082/TA-086 Modell handelte und die entsprechenden Schritte durchgeführt wurden.

3.03 Downgrader - (FW 20 Dec 2006)

Team NOOBz veröffentlichte interessanterweise nur etwa einen Monat nach Release einen Downgrader für 3.03 welcher den 8. Slot(Autoload) eines ungepatchten GTA: Liberty City Stories verwendete um mittels Goofy Exploit jedwede PSP auf FW 1.50 zu downgraden.

3.50 Downgrader - 26 Jun 2007 (FW 31 May 2007)

NOObz verwendet den Illuminati (Lumines) Exploit in Kombination mit einem 3.50 kernel exploit.

3.11 Downgrader - 10 Sep 2007 (FW 8 Feb 2007)

Da nicht jede PSP bis 3.50 geflasht werden kann veröffentlicht Fanjita diesen Downgrader, der wie der 3.50er den Illiminati Exploit verwendet.

Alle Firmwares bis 3.50 können entweder direkt oder über Umweg mit Firmware 1.50 geflasht werden. Mit Ausnahme des PSP 1007 Modells(Taiwan).

2.00 - 2.50 HEN

Die ersten HEN nutzten einen Exploit in GTA: LCS, welcher später bei der „Greatest Hits“ Version mit Firmware 2.60 gepatcht wurde. Der Exploit wurde „Goofy“ genannt.

2.00 - 2.71 HEN

Nachdem der TIFF exploit entdeckt wurde, wurden darauf basierende HEN veröffentlicht, welche auf jeder Firmware bis einschließlich 2.71 funktionierten.

3.00 - 3.03 HEN

Bis 3.03 war die Verwendung des Goofy Exploits nach wie vor möglich, dementsprechend wurden auch die passenden HEN veröffentlicht. Sony schloss danach auch auf Seiten der Firmware die Lücke und führte mit FW 3.30 einen weiteren IDStorage Check ein.

3.00 - 3.50 HEN

Später wurde der „Illuminati“ Exploit in Lumines gefunden, welcher erst mit 3.51 auf Seiten der Firmware gefixt wurde, auch auf den neueren UMDs ist dieser Exploit geschlossen.

5.03 HEN

- 15. April 2009: Davee veröffentlicht ein auf einem von ihm entdeckten libtiff Exploit basierendes Hello World, welches auf sämtlichen Modellen funktioniert.
- 6 Mai 2009: Davee veröffentlicht ChickHEN in Version 1, welches auf allen Modellen Homebrew für FW 5.03 ermöglicht. Es folgen einige Bugfix releases.
- Xenogears und Becus25 veröffentlichen ihren CFWEnabler, welcher das Laden von CFWs in den RAM ermöglicht, dies funktioniert erst seit Version 3.00 der HB auf dem 3000er Modell.
- Obwohl ChickHEN offiziell nur auf Version 5.03 funktioniert gibt es vereinzelte Berichte von glücklichen 5.05 Usern, der libtiff Exploit wurde in FW 5.50 gefixt.

Firmware 1.00

- April 2005: Durch einen DNS Trick im Content Downloader von Wipeout Pure ist es möglich, auf die UMD zu zuzugreifen, das EBOOT Format wird von NEM und dem „Saturn Expedition Committee“ reverse-engineered.
- Mai 2005: Hello World wird für FW 1.00 veröffentlicht, da bis dato keinerlei Checks des Codes vorhanden sind, lässt sich eben jener leicht mittels modifiziertem GCC und Binutils fabrizieren.
- Außerdem wurde es möglich UMDs zu dumpen und vom Memory Stick wie eine normale UMD zu starten.

Firmware 1.50

- 15. Juni 2005: Spanische Entwickler veröffentlichen Swaploit, vorm starten der gewünschten Homebrew Applikation wird der Memory Stick getauscht - nicht sehr stabil.

- Killer-X entwickelt den KXploit, welcher die sprintf Funktion verwendet um Homebrew zu starten, indem es zwei Ordner gibt, welche jener Applikation zugehörig sind, einer **abc** und der andere **abc%** benannt. Der % Ordner enthält nur ein Bild und die PARAM.SFO Datei, der andere eine zu EBOOT.PBP umbenannte DATA.PSP, die ausführbare Datei. Das Problem, dass nun pro Homebrew auch ein zweiter Eintrag mit korrupten Daten im XMB gelistet wird, wird entweder über einen Exploit im FAT16 System oder über das Namensschema %__SCE__name __SCE__name umgangen.

- No-KXploit Patch: Da die Verwendung zweier Ordner doch eher störend war, wurde der No-KXploit Patch entwickelt, eine Homebrew Applikation, welche die Firmware im RAM modifizierte und so den KXPloit für andere Programme unnötig machte, dieser Patch wurde später auch in die meisten Custom Firmwares integriert.

Werdegang der Custom Firmwares

Allgemeines

- Fokus der Slides liegt auf Dark Alex SE, OE und M33 Serien.
- Features welche in der Regel sämtliche Custom Firmware bietet:
    * Abspielen von ISO/CSO Images und Homebrew Applikationen
    * Zugriff auf den internen Flash.
    * Seit DAX OE Serie üblich: Recovery Menü
- Aufbau der klassischen CFWs: Teile des 1.50 Kernels in den der CFW gepatcht.
- Aufbau aktuellen CFWs: Es wird ein eigener IPL mitgeführt.

Custom Firmware 1.50 Proof of Concept

- 15 Jul 2006: Dark Alex veröffentlicht 1.50 POC, Features:
    * Autoboot
    * Ausführen von 1.00 FW Homebrew.
    * Einfacher Recovery Modus
- Es folgen einige darauf basierende Firmwares ohne nennenswerte Unterschiede.

Custom Firmware 1.53

- 19 Feb 2007: eiffel56 veröffentlicht die auf 1.50 POC basierende 1.53 neue Features:
    * Custom PRX Support
    * Verstecken von korrupten Menüeinträgen.
    * Starten von ISOs.
    * No-KXPloit Patch in die Firmware integriert.

Custom Firmware 2.71 SE - OFW 30 May 2006

- 8 Oct 2006: Dark Alex veröffentlicht 2.71 SE-A, welche die Kernels der Firmwares 1.50 und 2.71 vereint.
- 24 Oct 2006: 2.71 SE-B folgt und ermöglicht das spielen von CSO/ISO Images.
- 26 Oct 2006: 2.71 SE-B’ kommt und erspart das einlegen einer UMD für Spiele vom Stick.
- Wenige Tage später: 2.71 SE-B” ermöglicht das starten von Titeln, welche eigentlich die Version 2.80 benötigen.
- 2.71 SE-C ermöglichte es dann schließlich PRX Plugins zu laden.

Custom Firmware 3.02 OE - OFW 6 Dec 2006

- 21 Dec 2006: Dark Alex veröffentlicht 3.02 OE-A, welche die SE-C Features enthält, Flash und WMA Support bietet **und** das DRM des PSX Emulators bricht.
- 25 Dec 2006: 3.02 OE-B folgt und ermöglicht das spielen von selbst konvertierten PSX Titeln mit dem mitgelieferten popstation Utility vom Stick.

Custom Firmware 3.03 OE - OFW 20 Dec 2006

- 4 Jan 2007: Dark Alex veröffentlicht 3.03 OE-A, alle 3.02 OE-B Features sind enthalten, ferner lassen sich die PSX Titel nun auch komprimieren.
- 6 Jan 2007: 3.03 OE-A’ ermöglicht das einstellen von CPU/BUS Geschwindigkeit während des Spielens.
- 10 Jan 2007: 3.03 OE-B erforderte eine Installation von 3.03 OE-A im voraus, das Update ermöglichte das abspielen von H.264/MPEG-4 AVC—MP4-AVC Videos im Vollbild Modus(480x272).

Custom Firmware 3.03 OE - OFW 20 Dec 2006

- 25 Jan 2007: 3.03 OE-C war wieder ein größeres Update, die maximale Video Bitrate wurde von 768 kbit/s auf 16384 kbit/s erhöht, Wlan mit 333 MHz CPU ermöglicht, das verändern von CPU/BUS Geschwindigkeit im XMB ermöglicht und das Kaltstarten beschleunigt.

Custom Firmware 3.10 OE - OFW 30 Jan 2007

- 4 Feb 2007: 3.10 OE-A ermöglichte die Verwendung der 4. Helligkeitsstufe auch ohne angeschlossenes Netzteil, außerdem war das ausführen von statisch gelinkten ELF Dateien mit dem 3.10er Kernel möglich.
- 6 Feb 2007: 3.10 OE-A’ behob einen kleinen Bug bezüglich der aufgrund falsch statisch gelinkter Binaries das starten einiger Spiele verhinderte.

Custom Firmware 3.30 OE - OFW 28 Mar 2007

- 15 Apr 2007: Bis auf den Location Free Player sind sämtliche bisherigen CFW und OFW Features enthalten.
- 20 Apr 2007: 3.30 OE-A’ Sicherheitsupdate, welches einen Bug schließt, der Stellenweise das RAM überschreibt und so, wenn eine Stelle Kernel erwischt es mitunter schafft, die PSP zu bricken. Außerdem wurde das Autoboot Feature wird wieder eingeführt(fiel in 3.03 OE raus).

Custom Firmware 3.40 OE - OFW 20 Apr 2007

- 20 Apr 2007: Die selben Änderungen wie in der am selben Tag erschienen 3.30 OE-A’, außerdem überprüft der Installer nun, ob eine korrekte DATA.DXAR vorliegt.
- Kurz darauf kündigte Dark Alex an, sich zurückzuziehen...

Custom Firmware 3.51M33 - OFW 29 Jun 2007

- 14 Jul 2007: In der ersten Version sind sämtliche bisherigen CFW und OFW Features enthalten, angeblich wurde die OE Serie reverse engineered.
- 21 Jul 2007: In den vergangenen Tagen wurden 5 Updates, hauptsächlich mit Bugfixes released, das 6. und letzte offizielle M33 Update für diese Firmware erschien an diesem Tag.

Custom Firmware 3.52M33 - OFW 24 Jul 2007

- 25 Jul 2007: Bugfix von Go!Cam, GPS und sceKernelLoadExecVSH außerdem funktionieren gekaufte PSN Titel nun ebenfalls(in 3.51M33 und einigen OEs nicht möglich).
- 30 Jul 2007: Das erste Update erscheint, WLAN wurde verbessert, formatieren des flash1 und wiederherstellen der Einstellungen ist nun via Option möglich, 20MHz und 100MHz CPU Takt sind möglich, Hibernate/Power Off im USB Modus deaktiviert.

Custom Firmware 3.52M33 - OFW 24 Jul 2007

- Am 7. August wird ein interessantes Interview veröffentlicht [1].
- 19 Aug 2007: 3.52 M33-3 erscheint und liefert
  * USB Zugriff auf flash2 und flash3
  * 75 MHz und 133 MHz CPU Geschwindigkeit
  * VSH Menü
  * Unterstüzung für den 3.30 OE Popsloader

Es gibt einige Berichte mit diesem Update gebrickter PSPs...

[1] http://www.pspx.ru/forum/showthread.php?t=49651

Custom Firmware 3.52M33 - OFW 24 Jul 2007

...Grund dafür war, dass der Admin von ps3news.com anscheinend M33 Code in die Finger bekommen hatte, weswegen das Update PSPs, welche ps3news.com in der Browser History hatten, brickte.

- 21 Aug 2007: 3.52 M33-4 wird veröffentlicht:
    * Etliche Bugfixes
    * 75 MHz und 133 MHz CPU Geschwindigkeit nun via VSH Menü einstellbar.

Custom Firmware 3.60M33 - OFW 10 Sep 2007

- 10 Sep 2007: 3.60 M33 wird für die PSP 2000 veröffentlicht.
- Aufgrund von Motherboard Inkompatibilitäten enthalten die folgenden Firmwares keinen 1.50 Kernel.
- Die CFW musste mittels Pandora’s Battery installiert werden.

Custom Firmware 3.71M33 - OFW 13 Sep 2007

- 20 Sep 2007: Aufgrund eines weiteren Code Leaks kündigt Team M33 vorerst eine Pause an, 3.71M33 sei aber bereits fertig gestellt.
- 23 Sep 2007: Die Firmware wird veröffentlicht, mit dem Release treten die Köpfe hinter M33 hervor, es handelt sich um niemand geringeren als Dark Alex und Mathieulh.
    * 1.50 Add-On für die Fat enthalten
    * Durch etliche Änderungen in der Kernel API sind viele Plugins für ältere Firmware nichtmehr verwendbar.
- 2 Oct 2007: Version 2 des FW 1.50 Plugins und der Firmware mit einigen Bugfixes veröffentlicht.
- 8 Nov 2007: Version 3 bringt neben einigen Bugfixes auch einen überarbeiteten POPSLoader mit.
- 12 Dec 2007: Das 3. Update (-4) bringt Multi Disc Support für den POPSLoader.

Custom Firmware 3.80M33 - OFW 17 Dec 2007

- 14 Jan 2008: Die CFW bringt ein eigenes Netzwerk Update Feature mit, noch am selben Tag erscheint das erste Update, welches einen Fehler der *scePowerGetClockFrequencyInt* Funktion behebt.
- 16 Jan 2008: Das zweite und das dritte Update werden veröffentlicht.
- 20 Jan 2005: Das vierte Update (-5) wird veröffentlicht.

Custom Firmware 3.90M33 - OFW 29 Jan 2008

- 31 Jan 2008: Das Release der CFW überarbeitet das Netzwerkupdate und korrigiert IDS Schlüssel, das 1.50er Kernel Add-On wird am selben Tag veröffentlicht.
- 13 Feb 2008: Die 2. Version wird veröffentlicht, sie verbessert den Plugin Support und patcht den IPL in 2000er PSPs, so dass diese auch mit eingelegter Pandora’s Battery booten können.
- 30 Mar 2008: Das nächste Update folgt, es erhöht die Kompatibilität einiger Spiele zur Firmware.

Custom Firmware 4.01M33 - OFW 25 Jun 2008

- 28 Jun 2008: Mit dieser CFW wurde das übersetzen des Recovery Menüs ermöglicht, außerdem wurde ein Bug im VSH Menü in Kombination mit der PSPCam gefixt. Homebrew im GAME401 Ordner wird automatisch mit dem passenden 3.xx/4.xx Kernel gestartet.
- 29 Jun 2008: Die 2. Version wird veröffentlicht, sie patcht den selben *scePowerGetClockFrequencyInt* Bug wie 3.80 M33-2. Außerdem wird das Kernel 1.50 Add-On veröffentlicht.

Custom Firmware 5.00M33 - OFW 15 Oct 2008

- Die erste Version wird kurz nach erscheinen der Original Firmware veröffentlicht, sie behebt nur einen Bug, welcher die Taktrate beim Helligkeitslevel 0 zurück auf 222MHz setzt. Das 1.50 Kernel Modul folgt am nächsten Tag.
- 22 Oct 2008: Das erste Update behebt Probleme mit PSN/PSX Titeln, bringt einen neuen POPSLoader mit, es folgen Patches für den RAM Umgang im PSX Emu, das Netzwerk Update und die *sctrlKernelSetInit** Funktionen.

M33 Serie

- 5.00 M33-6 ist die letzte offizielle M33 Firmware
- Dark Alex zieht sich erneut aus der Szene zurück und nimmt leider auch seine Seite und das dazugehörige Forum vom Netz, was den Zugriff auf etliche PSP bezogene Dinge erschwert.

Pandora’s Battery - Die JigKick Battery und der Magic Memory Stick

Allgemeines

- Am 22 August 2007 von Team C+D veröffentlicht.
- Teilt sich in die JigKick Battery und den Magic Memory Stick auf.
- Bootet die PSP beim einlegen in den Service Mode und erlaubt das flashen beliebiger Daten auf den internen Flash sämtlicher PSP Modelle bis zum PSP 2000 Modell mit TA-088v3 Motherboard.

JigKick Battery

- Serial der Batterie wird auf 0xFFFFFFFF gesetzt
- Beim einlegen der JigKick Battery bootet die PSP vom 16. physischem Datenblock des Datenträgers (Magic Memory Stick) anstatt vom internen flash0.

Magic Memory Stick

- Das gewünschte Programm wird auf den Memory Stick entpackt und der zugehörige IPL auf den 16. Block geschrieben.
- Es können nur Memory Sticks des Pro Duo Typs bis zu einer Größe von 4GB zu Magic Memory Sticks konvertiert werden.
- Es ist möglich sämtliche PSP 1000 Modelle auf FW 1.50 zu flashen, oder auf alle Modelle bis zu jenen mit TA-088v3 Boards die M33 Firmwares ab Version 3.71M33 zu flashen, das starten vereinzelter Homebrew Applikationen ist ebenfalls möglich.

Sonstiges und Quellen

Zur Recherche/Verifizierung benutzt

- `http://alek.dark-alex.org/pspwiki/`
- `http://www.qj.net/`
- `http://www.portable-news.de/*`
- `http://www.pspsource.de/*`

Mit * markierte Adressen sind nicht sehr zuverlässig, zur Verifizierung einiger Daten dennoch geeignet.

Sonstiges

- 24c3 Talk
- Toolchain: svn://svn.ps2dev.org/psp/trunk/psptoolchain

Danke an sECuRE für den powerdot Tipp, AVGP, BadBoy_, Eiffel56 und Latino_Heat für Hinweise und Erinnerungen.