Custom Firmware

- CFW für Switch Version 1

CFW für Switch Version 1

Beschreibung:

Die Bootrom des Tegra X1 weist einen kritischen Defekt auf, bekannt als "Fusée Gelée", der im Tegra Recovery Mode auftritt. Der USB-Software-Stack umfasst eine Kopierfunktion, deren Umfang ein Angreifer bestimmen kann. Mithilfe eines eigens erstellten USB Control Request kann ein Angreifer diesen Mangel nutzen, um seine eigenen Daten in den Execution-Stack zu übertragen und somit kompletten Zugriff auf den Boot- und Powermanagement-Prozessor (BPMP) zu erlangen. Dies ermöglicht die vollständige Kontrolle über das Gerät, jedoch ist dazu physischer Zugriff erforderlich. Dieser Fehler wurde öffentlich bekannt, nachdem er am 24. April 2018 durchgesickert war.

Im Juli 2018 wurde das Problem durch eine aktualisierte Version der Switch behoben.

Vorrausetzungen:

Eure Switch muss den CPU Bug haben:

Hier der Seriennumemer check:

Seriennummern

TL;DR. Compare your serial here to know if your Switch is patched or not:

Serials beginning with XAW1:
Serials between XAW10000000000 - XAW10065000000 are safe to buy
Serials between XAW10066000000 - XAW10120000000 are possibly patched
Serials above XAW10120000000 are definitely patched

Serials beginning with XAW4:
Serials between XAW40000000000 - XAW40011000000 are safe to buy
Serials between XAW40011000000 - XAW40012000000 are possibly patched
Serials above XAW40012000000 are definitely patched

Serials beginning with XAW7:
Serials between XAW70000000000 - XAW70017500000 are safe to buy
Serials between XAW70017500000 - XAW70030000000 are possibly patched
Serials above XAW70030000000 are definitely patched

Serials beginning with XAJ1:
Serials between XAJ10000000000 - XAJ10020000000 are safe to buy
Serials between XAJ10020000000 - XAJ10030000000 are possibly patched
Serials above XAJ10030000000 are definitely patched

Serials beginning with XAJ4:
Serials between XAJ40000000000 - XAJ40044000000 are safe to buy
Serials between XAJ40044000000 - XAJ40083000000 are possibly patched
Serials above XAJ40083000000 are definitely patched

Serials beginning with XAJ7:
Serials between XAJ70000000000 - XAJ70040000000 are safe to buy
Serials between XAJ70040000000 - XAJ70050000000 are possibly patched
Serials above XAJ70050000000 and above definitely patched

Serials beginning with XAW9:
Refurbished Consoles directly from Nintendo. Possibly patched. However, data show a good percentage of unpatched consoles with this prefix.

Serials beginning with XAK:
No informations available, since those are only sold in Korea (?)

Serials beginning with XKW and XKJ:
These Switches have the new motherboard revision called "Mariko".
They are 100% patched.

Physikalisches Zubehör um das Leben leichter zu machen:

Einen JIG für den Home Button Recovery Modus (wenn du ein RCM-Loader hast, brauchst du keinen JIG, ist nämlich dabei):

Der komplizierteste Teil dieses Vorgangs besteht darin, den Tegra Recovery Mode zu aktivieren. Dafür müssen die Tasten POWER, Lautstärke hoch und HOME gleichzeitig gedrückt werden, während die Switch ausgeschaltet ist. Allerdings besitzt die Switch selbst keinen HOME-Button; dieser befindet sich nur an den Controllern. Stattdessen ist der HOME-Button bei der Switch über Pin 10 am Connector des rechten Joy-Con angebunden.

Um eine Verbindung herzustellen, können Sie entweder mit einer Büroklammer Pin 1 und Pin 10, also die beiden äußeren Pins, oder mit einem Kabel Pin 10 und Pin 1 verbinden. Alternativ zu Pin 1 können auch die oberen Kühlrippen, die Rail selbst oder die nahegelegene Schraube verwendet werden. Wichtig ist, dass Pin 10 dabei geerdet wird.

Oder man nutzt einen JIG was ich nur empfehlen kann:
Diesen einfach and er rechten seite mit on noch unten reinschieben wo sonst der Controller reinkommt.
Dann die Switch an den Computer oder den RCM Loader anschließen und die Switch starten.
Per Computer muss dann noch ein Payload gesendet werden. Am RCM Loader wird ja mittels Plus taste die Firmware ausgewählt. Dazu unten später. Erst nach dem auswählen die Switch starten.

https://www.amazon.de/rcm-jig/s?k=rcm+jig

Ein RCM Loader One :

https://www.amazon.de/RCM-Loader-kompatibel-Nintendo-Switch/dp/B0C7KJ737C/

RCM Loader bei eBay

Und wozu das Ding? Payloads können doch auch vom Computer direkt gesnedet werden
Hier ein beschreibung im Spoiler:

Vorteile RCMLoader vs Payload Software

Payloads können auch direkt von einem Computer aus gesendet werden, um den Recovery Mode (RCM) einer Nintendo Switch zu nutzen. Hier sind einige Vor- und Nachteile dieser beiden Methoden, also das Senden von Payloads vom Computer und das Verwenden eines dedizierten Geräts wie dem RCM Loader:

Payloads vom Computer senden

Vorteile:

1. **Keine zusätzliche Hardware erforderlich**: Wenn du bereits einen Computer hast, brauchst du kein zusätzliches Gerät zu kaufen.

2. **Flexibilität**: Du kannst verschiedene Payloads leicht austauschen und anpassen, da du direkten Zugriff auf die Dateien auf deinem Computer hast.
3. **Updates und Support**: Es ist einfacher, Software auf dem Computer zu aktualisieren und Support für gängige Payload-Software zu finden.

Nachteile:

1. **Komplexität**: Für Anfänger kann es komplizierter sein, die erforderliche Software einzurichten und zu konfigurieren.
2. **Portabilität**: Ein Laptop oder Desktop-PC ist weniger tragbar als ein kleiner, dedizierter Loader.
3. **Abhängigkeit vom Betriebssystem**: Manchmal können Kompatibilitätsprobleme mit bestimmten Betriebssystemen oder spezifischen Softwareversionen auftreten.

Verwendung eines RCM Loaders

Vorteile:

1. **Portabilität**: Der RCM Loader ist klein, leicht und kann leicht transportiert werden, was ihn ideal für Modifikationen unterwegs macht.
2. **Einfache Bedienung**: Einmal eingerichtet, ist der Loader oft einfacher zu bedienen, da er in der Regel nur das Anschließen an die Konsole erfordert, ohne weitere Konfiguration.
3. **Unabhängigkeit**: Der Loader ist nicht abhängig von einem Computer oder einer speziellen Software, was ihn in verschiedenen Situationen nützlich macht.

Nachteile:

1. **Kosten**: Ein RCM Loader ist eine zusätzliche Investition, da es sich um ein spezielles Gerät handelt.
2. **Eingeschränkte Funktionalität**: Im Vergleich zu einem Computer, der regelmäßig aktualisiert und angepasst werden kann, bietet der Loader möglicherweise nicht dieselbe Flexibilität oder Unterstützung für die neuesten Payloads und Updates.

Zusammenfassung

Die Entscheidung, ob du Payloads direkt von einem Computer sendest oder einen RCM Loader verwendest, hängt von deinen spezifischen Bedürfnissen ab. Wenn Portabilität und einfache Bedienung entscheidend sind, könnte ein RCM Loader die bessere Wahl sein. Wenn du jedoch Wert auf Flexibilität und keine zusätzlichen Kosten legst, könnte das Senden von Payloads vom Computer die bessere Option sein.

Eine SD Karte

Denn irgendwo muss die Firmware und Homebrews ja drauf.
Nintendo unterstützt SD-Karten in den Dateiformaten **FAT32 oder exFAT**.
unsere Custom Firmware unterstützen **nur** **FAT32**
Das Partitionslayout mus mbr / msdos haben.
Also mit **FAT32** formatieren.

Der SD-Kartenslot befindet sich unter dem Ständer.

Ein Payload allein reicht nicht.
Es muss auch eine Firmware auf die SD-Karte

Hier nehmen wir asl Beispiel Hekate + Atmosphere

Hekate : https://wiidatabase.de/switch-downloads/custom-firmware/hekate/?dl=0

Atmosphere : https://wiidatabase.de/switch-downloads/custom-firmware/atmosphere/?dl=0
hekate INI, das ist das Pendant zur Windows boot.ini / bcd, da steht drin welche Firmware geladen werden soll.
Diese Ini Datei in das Verzeichnis bootloader einfügen und überschreiben

Ini : https://wiidatabase.de/switch-downloads/custom-firmware/hekate/?dl=1

Möchte man die Signatürprüfung deaktivieren, anstatt die erste INI diese die ganze ZIP auf die SD KArte kopieren und überschreiben sagen. Die Zip Atmosphere muss schon auf der SD-Karte sein.

https://wiidatabase.de/switch-downloads/hacks/signatur-patches/?dl=0

Den Inhalt einfach auf die SD Karte entpacken / kopieren.

Software Voraussetzungen wenn kein RCM Loader verwendet wird:

Der Python fusee-launcher.py für Linux und Mac

https://static.wiidatabase.de/fusee-launcher.zip

Installation unter Linux
Hardware Vorausetzung:
xHCI-Controller verfügen (USB 3.0 oder jeder andere USB-Port an einem modernen System).

```
apt install python3 python3-pip
pip install pyusb
```

Installtion unter Mac
keine Hardware Vorausetzungen

Python3 auf MACOS installieren.

```
pip install pyusb
```

oder für Windows

TegraRcmGUI -> https://github.com/eliboa/TegraRcmGUI

Payload durchführen

Mittels RCMLoader

Der RCM Loader kommt mit einigen Firmwares von Haus aus mit.

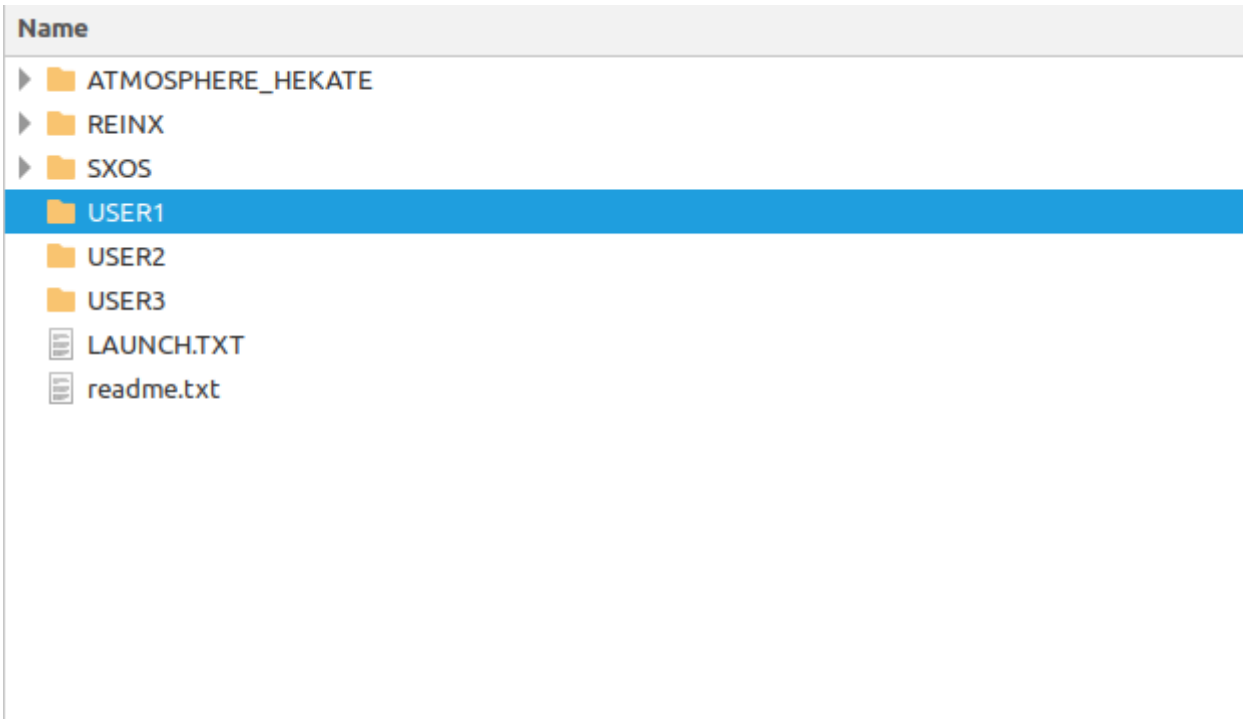
Mittels + Taste Können die Firmwares gewählt werden am Gerät.
Die + Taste gedrückt halten dann wird der aktuelle Modus angezeigt , dann nochmals gedrückt halten dann wird die nächste Farbe angewählt, nochmals gedrückt halten wieder die nächste usw. Diese sind:

LED-color	Folder name	Bulit-in payload
1 Blue	ATMOSPHERE_HEKATE	□□□HEKATE_CTCAER_5.6.0_Nyx_1.0.6
2 Green	REINX	REINX_3.0
3 Red	SXOS	SX_loader_1.0
4 Yellow	USER1	-
5 Magenta	USER2	-
6 Cyan	USER3	-

Die readme.txt-Datei vermerkt das Datum der letzten Update-Durchführung und die integrierten Payloads inklusive ihrer jeweiligen Farben (siehe Tabelle oben). Auf unserem Dongle war die Bezeichnung "USER1" in "USER1_XKOS" geändert und enthielt XKOS, eine Kopie von SX OS. Überflüssig zu sagen, dass ich dies sofort entfernte und den Ordner umbenannte. Die Datei "LAUNCH.TXT" listet den aktuell eingestellten Payload auf.

In jedem Verzeichnis befindet sich eine Datei "payload.bin", die durch andere Payloads ersetzt werden kann, beispielsweise bei der Veröffentlichung einer neuen Version von ReiNX, um den Payload zu aktualisieren. Die "USER"-Verzeichnisse sind dafür gedacht, eigene Payloads aufzunehmen.

Gelegentlich wird eine neue Firmware veröffentlicht. In diesem Fall muss die aktuelle Version heruntergeladen und in den "IAP"-Ordner auf dem Dongle kopiert werden. Nachdem der Dongle getrennt und erneut verbunden wurde, startet nach drei Sekunden automatisch die Aktualisierung, woraufhin der Ordner gelöscht wird.



Start des Payloads. Mittels + die Firmware auswählen und und warten

Mittels Software

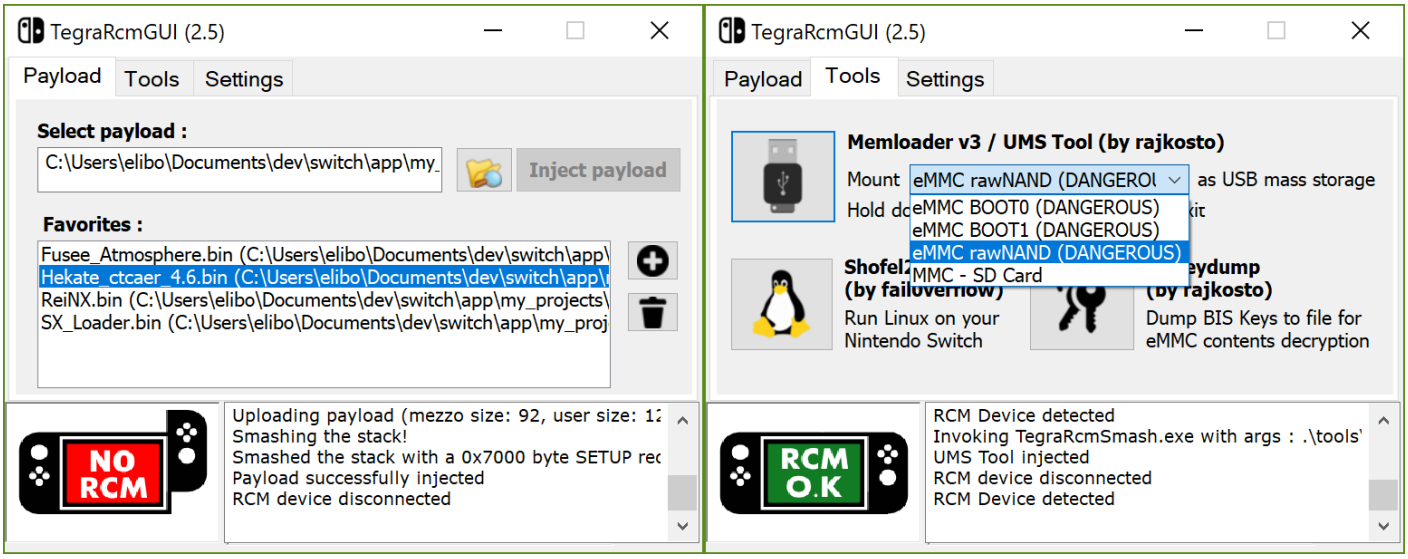
Die Switch in den RCM Modus setzten.
Den JIG Einsetzten und Erst Lautstärke hoch dann gedrückt halten und dazu Power drüken.
Dann mit USB Kabel mit dem Computer / MAC verbinden

fusee-launcher.py

```
python fusee-launcher.py PFAD_ZUM_PAYLOAD.bin
```

Über die Windows Software

Paxload durchsuchen und unter tools Memloader v3 auswählen.


TegraRcmGUI (2.5)
Payload
Tools
Settings
Select payload :
C:\Users\elibo\Documents\dev\switch\app\my_
Inject payload
Favorites :
Fusee_Atmosphere.bin (C:\Users\elibo\Documents\dev\switch\app\
Hekate_ctcaer_4.6.bin (C:\Users\elibo\Documents\dev\switch\app\
ReiNX.bin (C:\Users\elibo\Documents\dev\switch\app\my_projects\
SX_Loader.bin (C:\Users\elibo\Documents\dev\switch\app\my_proj
NO RCM
Uploading payload (mezzo size: 92, user size: 12
Smashing the stack!
Smashed the stack with a 0x7000 byte SETUP rec
Payload successfully injected
RCM device disconnected
TegraRcmGUI (2.5)
Payload
Tools
Settings
Memloader v3 / UMS Tool (by rajkosto)
Mount
eMMC rawNAND (DANGEROU
as USB mass storage
eMMC BOOT0 (DANGEROUS)
eMMC BOOT1 (DANGEROUS)
eMMC rawNAND (DANGEROUS)
MMC - SD Card
Run Linux on your
Nintendo Switch
Dump BIS Keys to file for
eMMC contents decryption
RCM O.K
RCM Device detected
Invoking TegraRcmSmash.exe with args : .\tools
UMS Tool injected
RCM device disconnected
RCM Device detected