

Modification LK.bin to erease Orange state and confirmation boot

Bypass Confirmation Boot

Tool necessary : Ghidra

Download and install here : <https://github.com/NationalSecurityAgency/ghidra>

Open file lk.bin in Ghidra

- File --> new project
- Non-Shared Project --> Next

image.png

- Give a name to your project --> Next

image.png

- File --> import File
- Import File lk.bin you want patch

image.png

- Select Langage --> ARM v7 | 32 | little | default

image.png

image.png

- Double click on file

image.png

- respond yes to analyzed

image.png

- We will get

image.png

- Search --> for String

image.png

- continue with clicking on Search

image.png

- type "dm-verity corruption" on filter

image.png

- One final will find --> click on line find

image.png

- this will give

image.png

- Go to the fonction who call the string "dm-verity corruption" with double click on hexa (FUN_00056c40:00056c8e)

image.png

- This will give

image.png

- We get the fonction we need on right

image.png

- The fonction who call string dm-verity is highlighted

image.png

- We can understand if the boot not start correctly

the var `image.png` and give `image.png__`

so the first an green is if boot is corectly and an red if we got an error

image.png

- We therefore need to modify one of these variables so that it is no longer used in the function.

`image.png` or `image.png__`

- In the function, if we click on the desired variable, we move to the line where it is in the file.

image.png

- Right Click on line --> Patch instruction

- Change value of condition

[image.png](#)

- We can do like this

[image.png](#)

[image.png](#)

- After this we can save file quit
- For export with menu project
- Right click on file --> select export
- You can choose Format Original File

Find the warning string

<https://github.com/R0rt1z2/lkpatcher>

<https://lkpatcher.r0rt1z2.com/>

<https://blog.r0rt1z2.com/patch-mediatek-bootloader-images-lk.html>

Revision #5

Created 2024-04-22 08:36:27 UTC by Foufure

Updated 2024-05-23 13:20:09 UTC by Foufure