17/11/2024

CP Plus

Security Assessment Report

CP-XR-DE21-S -4G Router
Firmware version 1.031.022

Company Details

Company Name	CPPLus - Aditya Infotech Ltd.(CP PLUS)
Email	support@cpplusworld.com
Telephone	+91-8800952952

Document History

Version	Date	Author	Remark
1.0	17/11/2024	Yashodhan	First Draft

Security Assessment Details

1.1 Executive Summary

Security Assessment of **CP-XR-DE21-S -4G Router** - **Firmware version 1.031.022** model has been performed, considering below common security issues:

- ✔ If any Hardware debug ports are open.
- ✔ If any device logs are accessible to third person
- ✔ If proper access control is implemented across the device.
- ✔ If proper Authorization & Authentication System is implemented.

Overall security postures of the device are good, though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application.
The security assessment revealed 1 medium severity issue in this product.

The consolidated summary of the assessment has been presented in the Executive Summary section. Additional information is contained within the Detailed Vulnerability Information section of this report.

1.2 Scope and Objectives

The scope of this assessment was limited to Hardware, Firmware and Wireless Communication of CP-XR-DE21-S -4G Router .

1.3 Technology Impact Summary

The security assessments on the Hardware, Firmware and Wireless communication has been performed. These assessments aim is to uncover any security issues in the assessed 4G router explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.
It was identified that CP-XR-DE21-S -4G Router is having UART port open to read the boot logs.

- ► An attacker can read boot logs such as BLE connection event, firmware version and sensor data from UART port

1.4 Business Impact Summary

Following is the business impact

- The boot logs and sensor data on UART is threat to IP of the product from the business competitors.

1.5 Testing Environment and Tools

To perform hardware security assessment over the CP-XR-DE21-S -4G Router hardware tools such as USB-UART converter, Picocom utility.

1.6 Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	CVSS String	Severity	Status
CP-XR-4G-01	Hardware	UART Port Exposing Serial Logs	6.7	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:H/SI:N/SA:N	Medium	Not Fixed

1.7 Device Strengths

Not discussed.

1.8 Device Weakness

The below mentioned vulnerabilities were identified during the process of Hardware security testing.

- The device logs can be accessible over UART port

Technical Findings

2.1 CP-XR-4G-01: UART Port Exposing Serial Logs

Potential Impact : MEDIUM

Description :

During the assessment it was identified that whenever logs from UART port are accessible that includes boot logs, hardware addresses, register dump,

Affected Hosts : UART Port, Device boot.

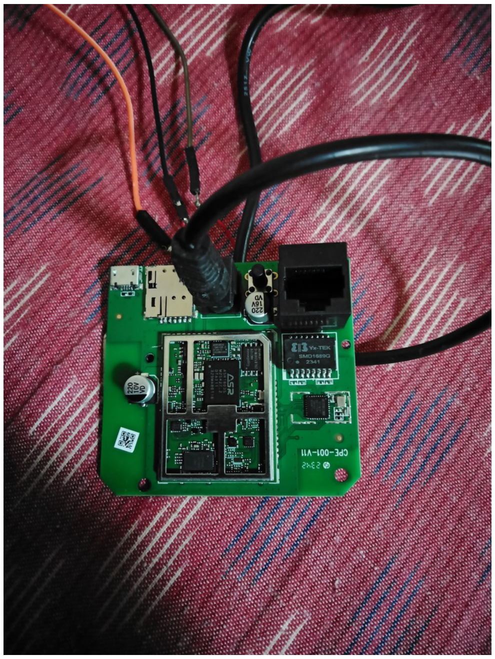
Technical Risk : The technical sensor parameters sensed and calculated by device are can be accessed in original data transmission format

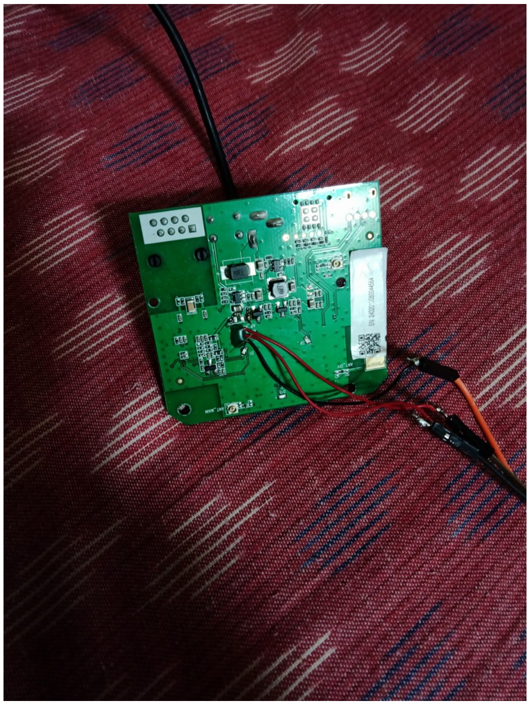
Business Risk : By understanding the log structure, the malicious actor can craft the malicious payload and bypass boot or firmware update.

Mitigations : In the final production the UART logs can be disabled.

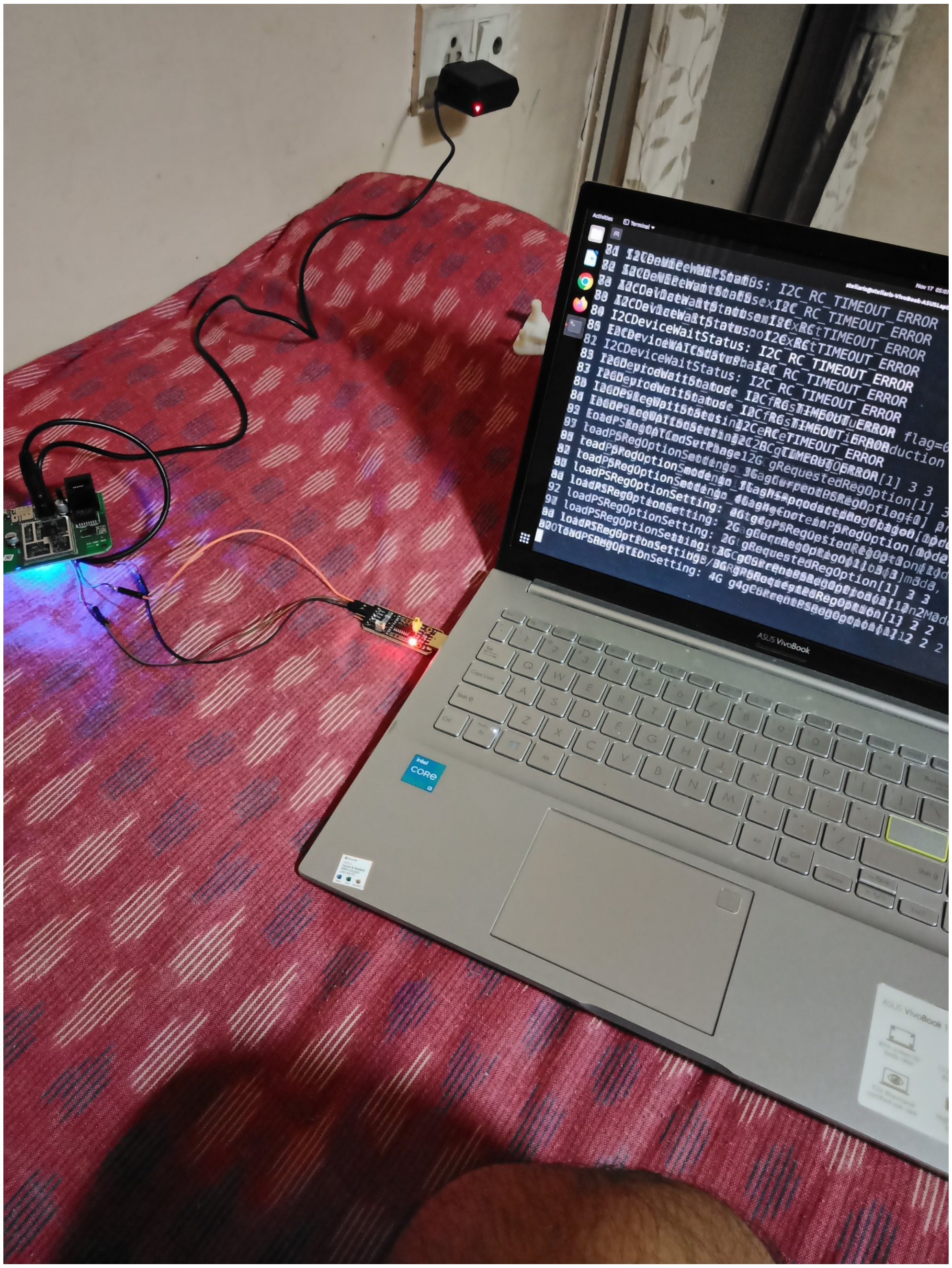
Steps to Reproduce:

1. Disassemble the CP-XR-DE21-S -4G Router and find UART pins viz 3.3 V, Gnd,TX and RX as shown in next image.



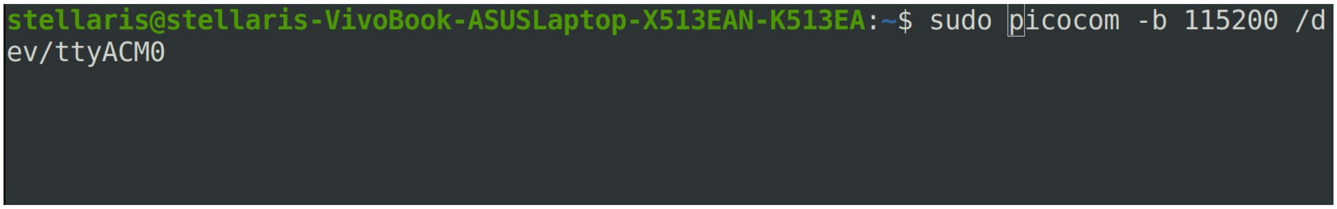


2. Solder the pins and connect to USB to UART Converter and connect to laptop as shown in image



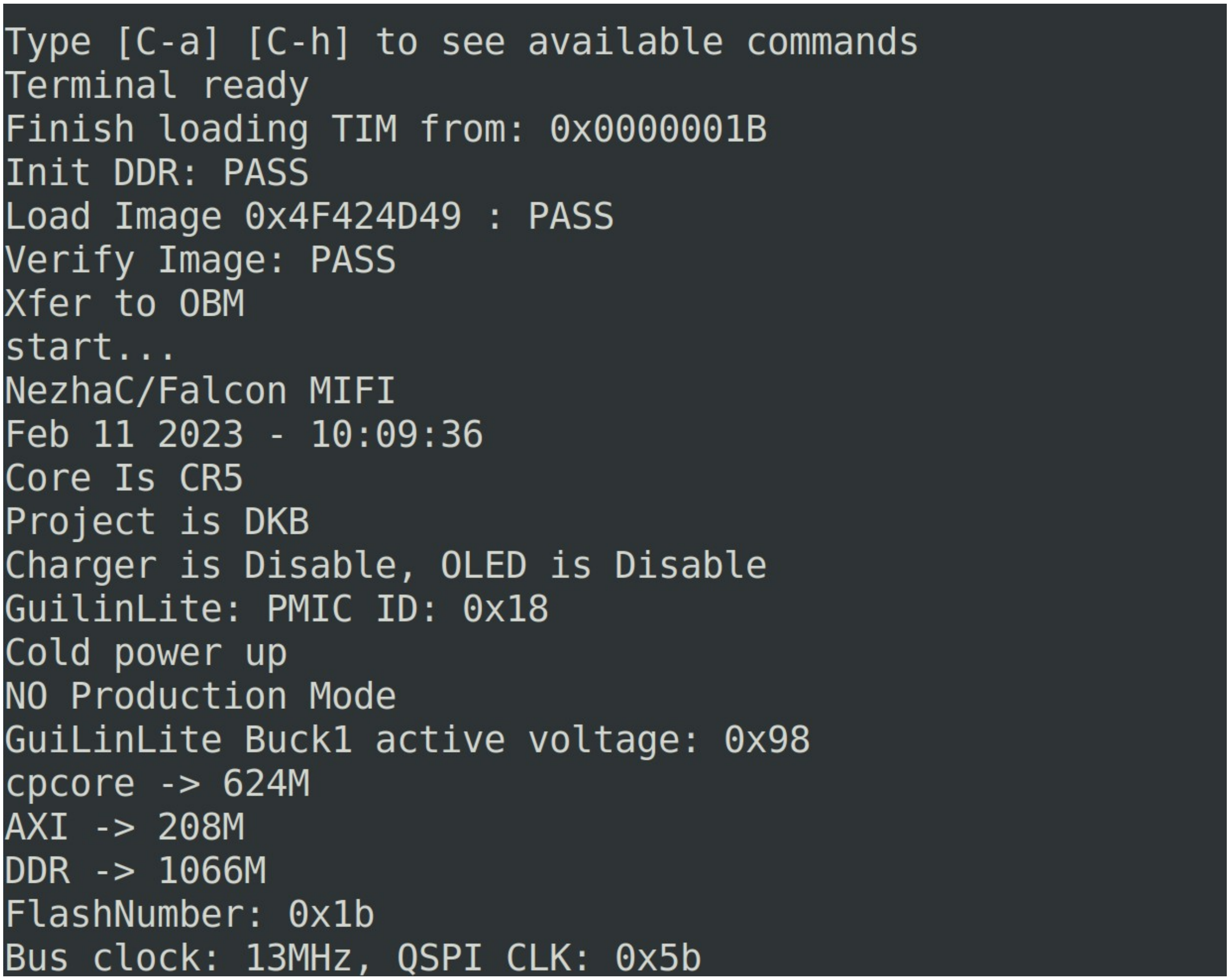
```
81 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
82 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
80 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
80 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
80 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
80 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
82 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
83 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
83 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
80 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
80 I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR flag=0
92 loadPSRegOptionSetting: I2C_RC_TIMEOUT_ERROR duction
97 loadPSRegOptionSetting: I2C_RC_TIMEOUT_ERROR
80 loadPSRegOptionSetting: 2G gRequestedRegOption[1] 3 3
82 loadPSRegOptionSetting: 3G gCurrentPSRegOption[1] 3
80 loadPSRegOptionSetting: 4G gCurrentPSRegOption[0] 0
80 loadPSRegOptionSetting: 4G gCurrentPSRegOption[0] mode
92 loadPSRegOptionSetting: 2G gRequestedRegOption[1] mode
97 loadPSRegOptionSetting: 2G gRequestedRegOption[1] mode,
80 loadPSRegOptionSetting: 3G gRequestedRegOption[1] 3 3
80 loadPSRegOptionSetting: 4G g4gCurrentPSRegOption[1] 2 2
```

3. Run picocom serial utility on terminal as shown below

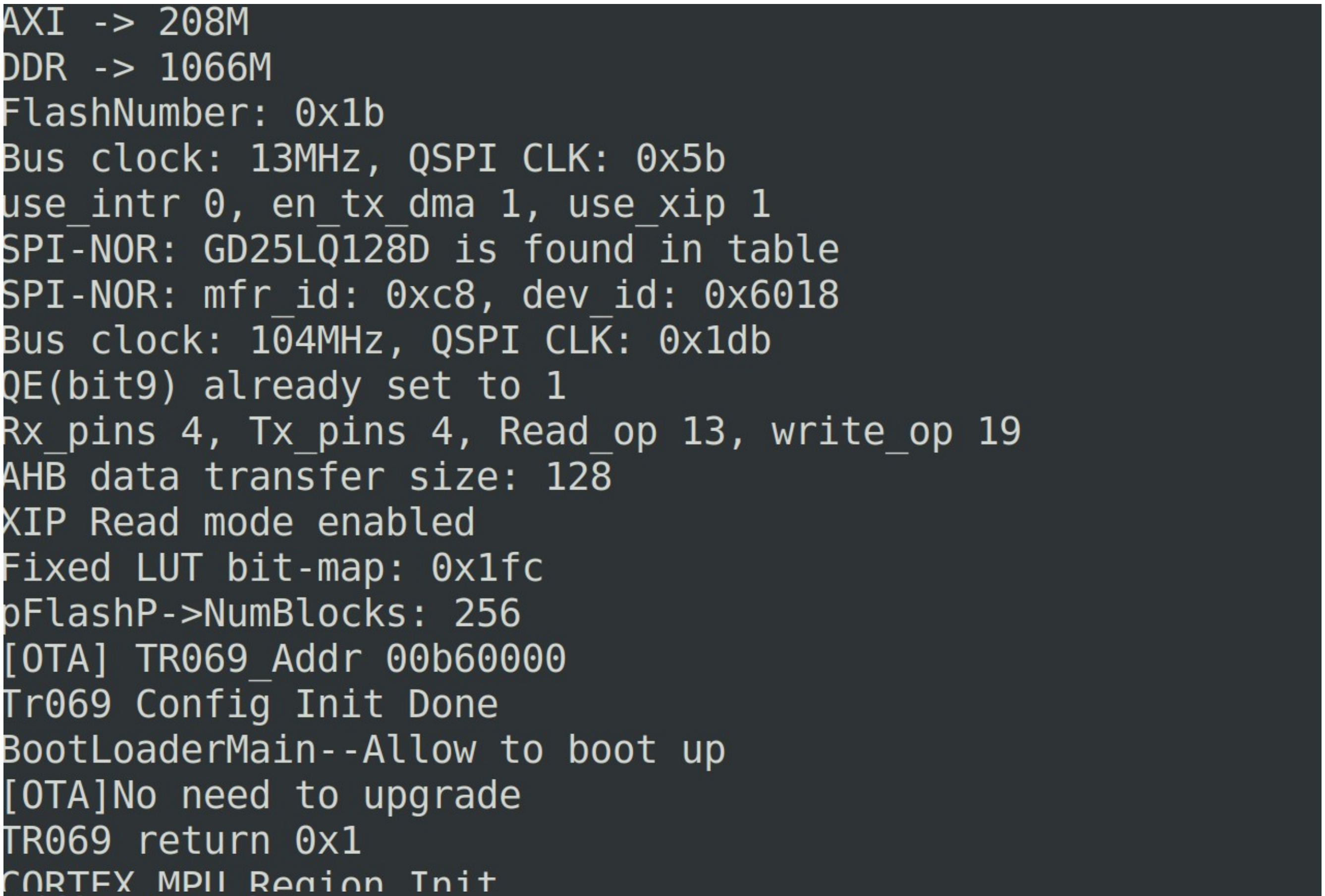


```
stellaris@stellaris-VivoBook-ASUSLaptop-X513EAN-K513EA:~$ sudo picocom -b 115200 /d
ev/ttyACM0
```

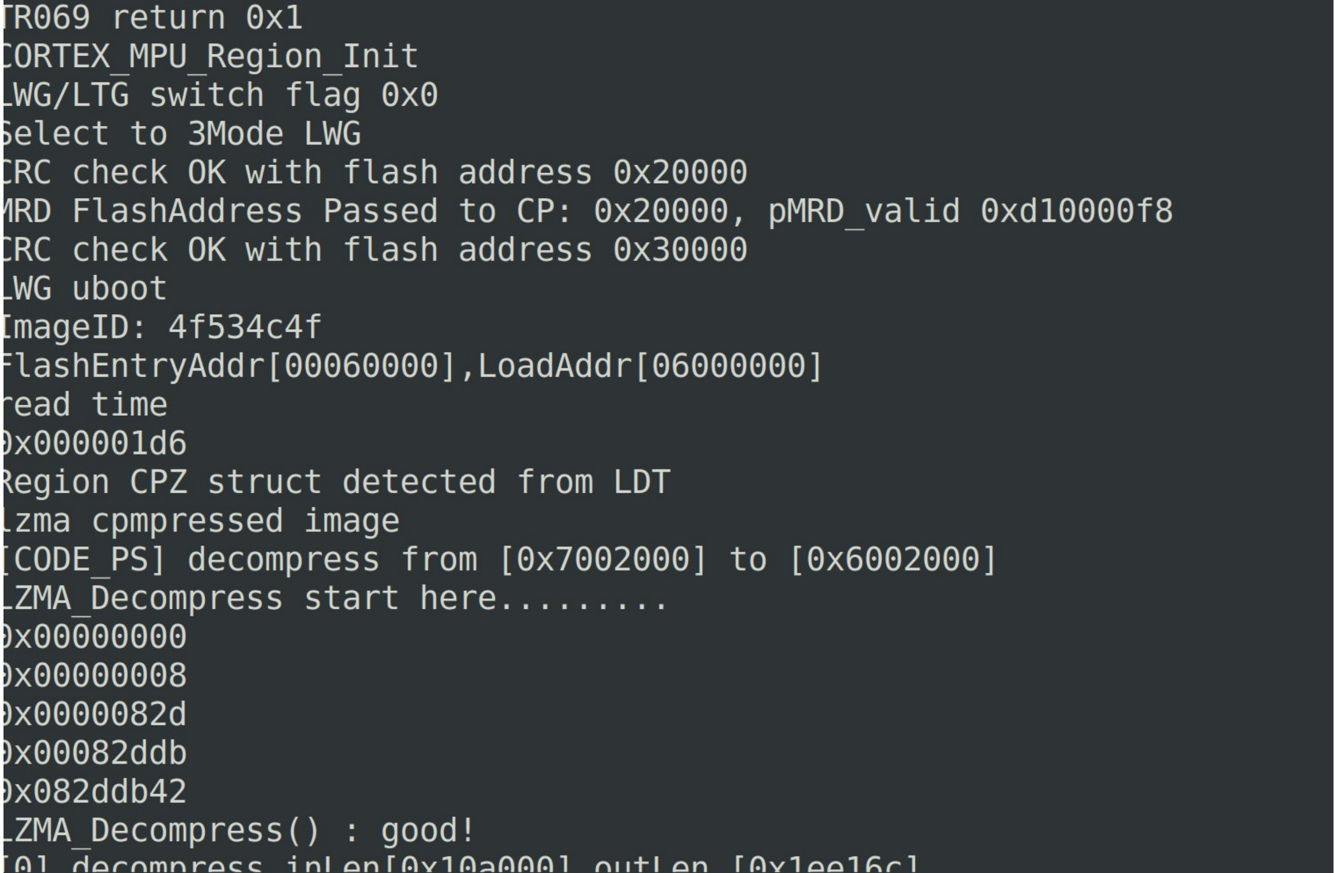
4. Below are the logs available that discloses information over UART port showing the vulnerability after accessing UART data over Picocom.



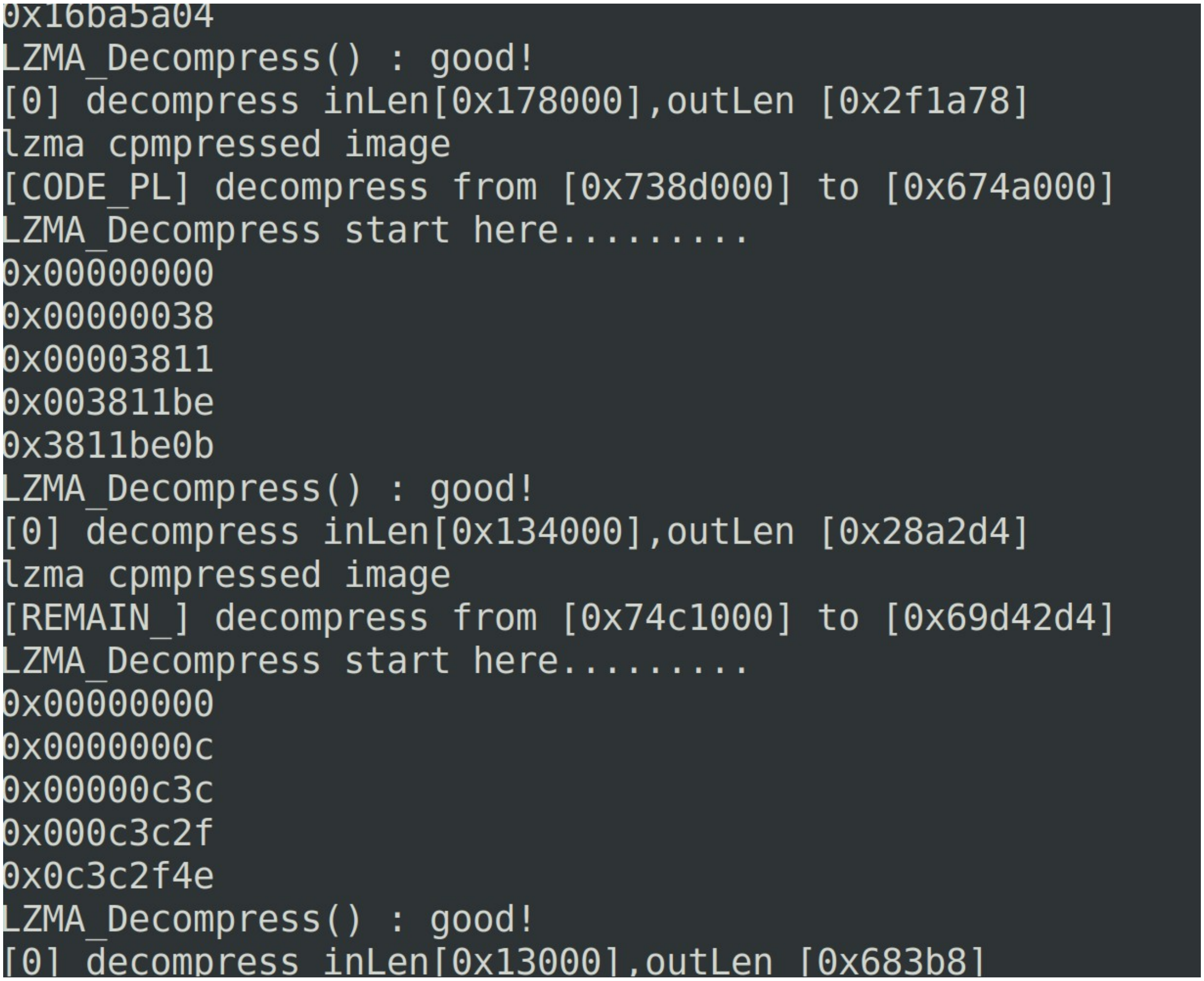
```
Type [C-a] [C-h] to see available commands
Terminal ready
Finish loading TIM from: 0x0000001B
Init DDR: PASS
Load Image 0x4F424D49 : PASS
Verify Image: PASS
Xfer to OBM
start...
NezhaC/Falcon MIFI
Feb 11 2023 - 10:09:36
Core Is CR5
Project is DKB
Charger is Disable, OLED is Disable
GuilinLite: PMIC ID: 0x18
Cold power up
NO Production Mode
GuiLinLite Buck1 active voltage: 0x98
cpcore -> 624M
AXI -> 208M
DDR -> 1066M
FlashNumber: 0x1b
Bus clock: 13MHz, QSPI CLK: 0x5b
```



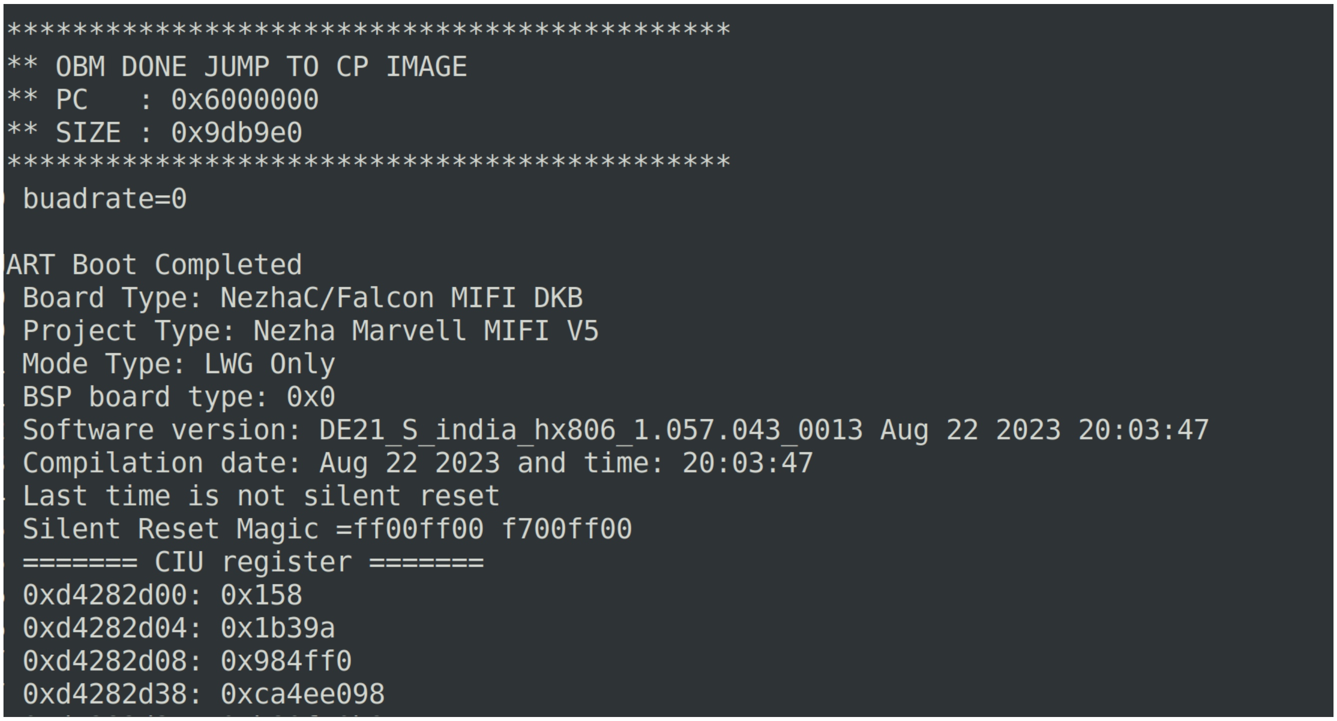
```
AXI -> 208M
DDR -> 1066M
FlashNumber: 0x1b
Bus clock: 13MHz, QSPI CLK: 0x5b
use_intr 0, en_tx_dma 1, use_xip 1
SPI-NOR: GD25LQ128D is found in table
SPI-NOR: mfr_id: 0xc8, dev_id: 0x6018
Bus clock: 104MHz, QSPI CLK: 0x1db
QE(bit9) already set to 1
Rx_pins 4, Tx_pins 4, Read_op 13, write_op 19
AHB data transfer size: 128
XIP Read mode enabled
Fixed LUT bit-map: 0x1fc
pFlashP->NumBlocks: 256
[OTA] TR069_Addr 00b60000
Tr069 Config Init Done
BootLoaderMain--Allow to boot up
[OTA]No need to upgrade
TR069 return 0x1
CORTEX_MPU_Region_Init
```



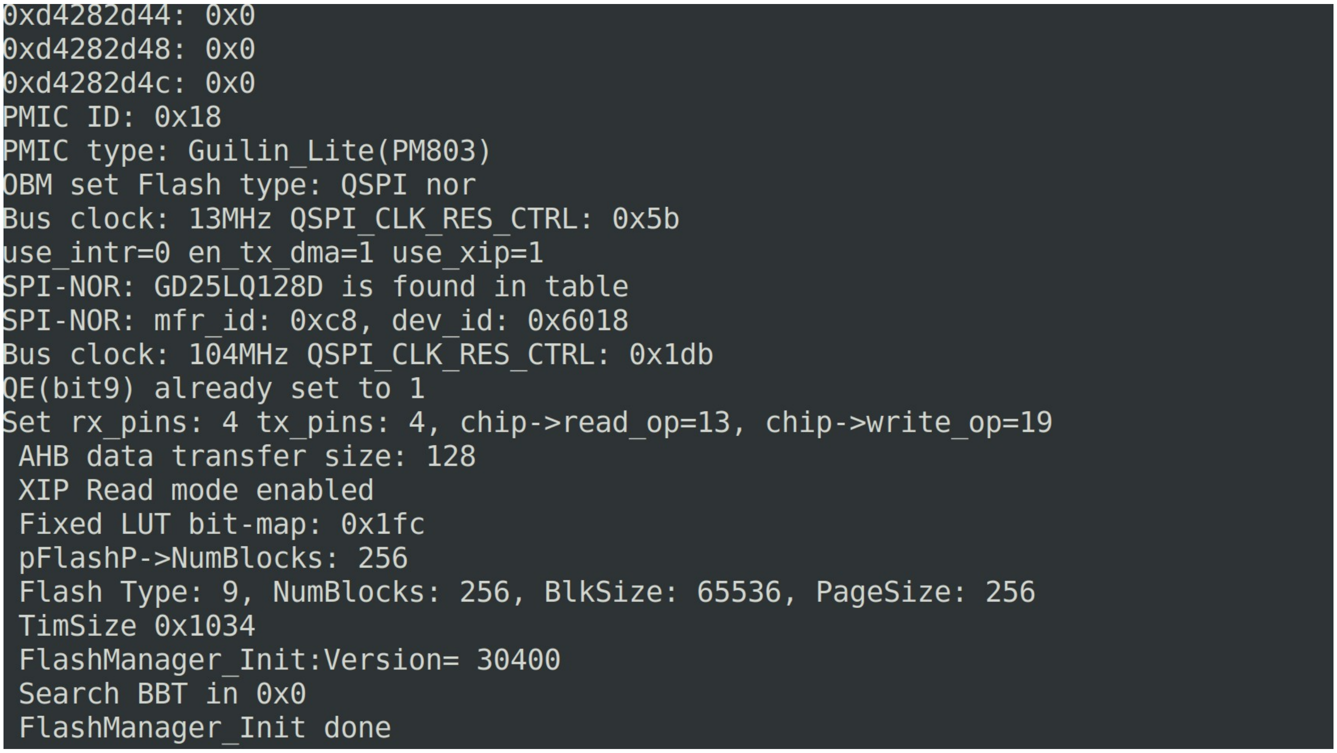
```
TR069 return 0x1
CORTEX_MPU_Region_Init
LWG/LTG switch flag 0x0
Select to 3Mode LWG
CRC check OK with flash address 0x20000
MRD FlashAddress Passed to CP: 0x20000, pMRD_valid 0xd10000f8
CRC check OK with flash address 0x30000
LWG uboot
ImageID: 4f534c4f
FlashEntryAddr[00060000],LoadAddr[06000000]
read time
0x000001d6
Region CPZ struct detected from LDT
lzma cpmpressed image
[CODE_PS] decompress from [0x7002000] to [0x6002000]
LZMA_Decompress start here.........
0x00000000
0x00000008
0x0000082d
0x00082ddb
0x082ddb42
LZMA_Decompress() : good!
[0] decompress inLen[0x10a000] outLen [0x1ee16c]
```



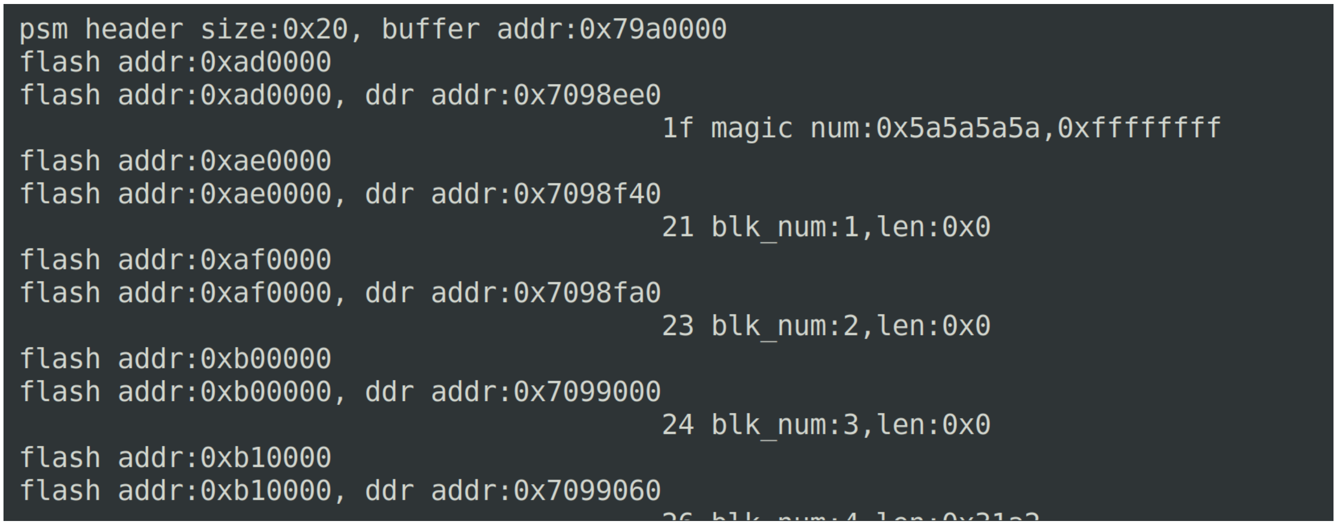
```
0x16ba5a04
LZMA_Decompress() : good!
[0] decompress inLen[0x178000],outLen [0x2f1a78]
lzma cpmpressed image
[CODE_PL] decompress from [0x738d000] to [0x674a000]
LZMA_Decompress start here.........
0x00000000
0x00000038
0x00003811
0x003811be
0x3811be0b
LZMA_Decompress() : good!
[0] decompress inLen[0x134000],outLen [0x28a2d4]
lzma cpmpressed image
[REMAIN_] decompress from [0x74c1000] to [0x69d42d4]
LZMA_Decompress start here.........
0x00000000
0x0000000c
0x00000c3c
0x000c3c2f
0x0c3c2f4e
LZMA_Decompress() : good!
[0] decompress inLen[0x13000],outLen [0x683b8]
```



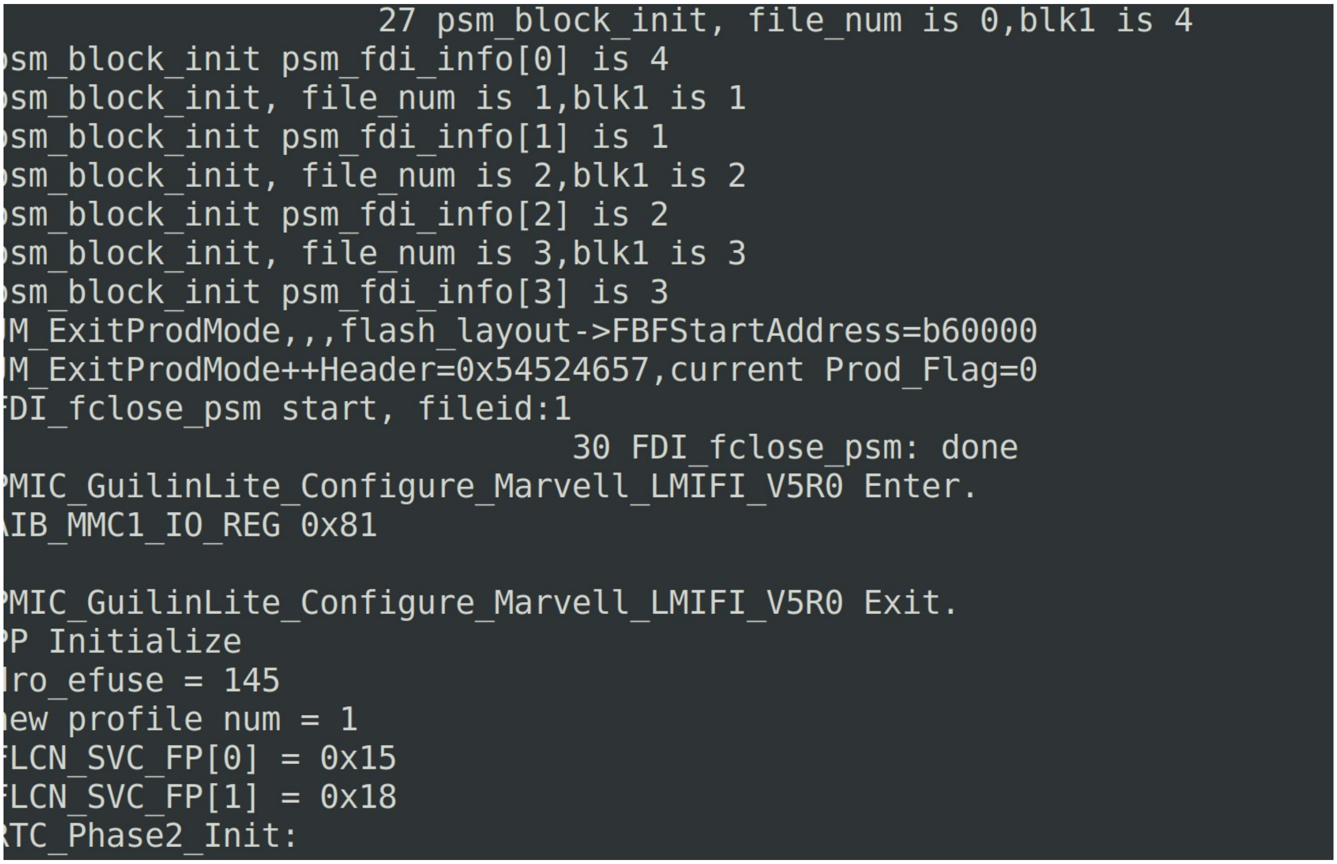
```
********************************************
** OBM DONE JUMP TO CP IMAGE
** PC   : 0x6000000
** SIZE : 0x9db9e0
********************************************
 buadrate=0

ART Boot Completed
 Board Type: NezhaC/Falcon MIFI DKB
 Project Type: Nezha Marvell MIFI V5
 Mode Type: LWG Only
 BSP board type: 0x0
 Software version: DE21_S_india_hx806_1.057.043_0013 Aug 22 2023 20:03:47
 Compilation date: Aug 22 2023 and time: 20:03:47
 Last time is not silent reset
 Silent Reset Magic =ff00ff00 f700ff00
 ======= CIU register =======
 0xd4282d00: 0x158
 0xd4282d04: 0x1b39a
 0xd4282d08: 0x984ff0
 0xd4282d38: 0xca4ee098
```



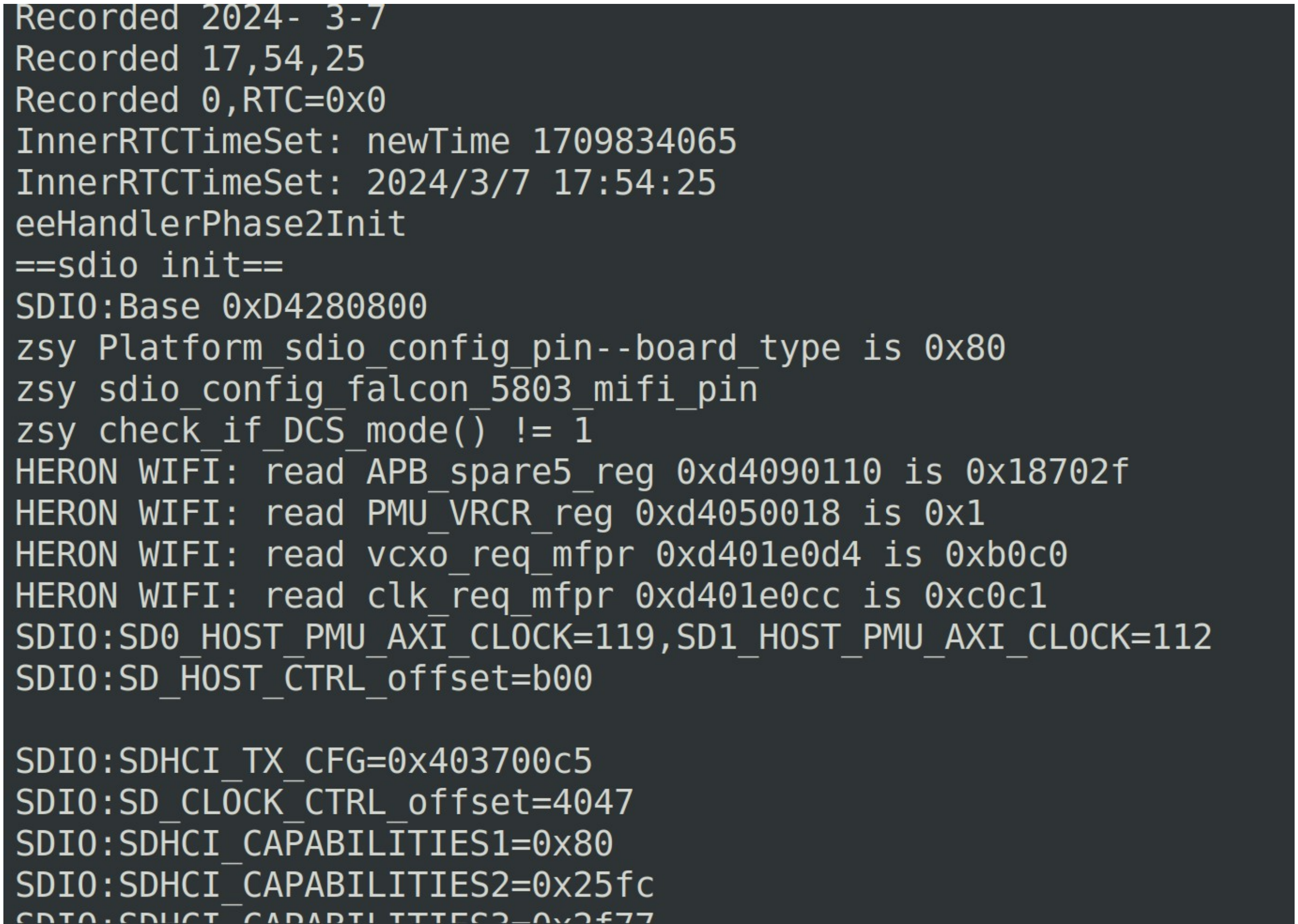
```
0xd4282d44: 0x0
0xd4282d48: 0x0
0xd4282d4c: 0x0
PMIC ID: 0x18
PMIC type: Guilin_Lite(PM803)
OBM set Flash type: QSPI nor
Bus clock: 13MHz QSPI_CLK_RES_CTRL: 0x5b
use_intr=0 en_tx_dma=1 use_xip=1
SPI-NOR: GD25LQ128D is found in table
SPI-NOR: mfr_id: 0xc8, dev_id: 0x6018
Bus clock: 104MHz QSPI_CLK_RES_CTRL: 0x1db
QE(bit9) already set to 1
Set rx_pins: 4 tx_pins: 4, chip->read_op=13, chip->write_op=19
 AHB data transfer size: 128
 XIP Read mode enabled
 Fixed LUT bit-map: 0x1fc
 pFlashP->NumBlocks: 256
 Flash Type: 9, NumBlocks: 256, BlkSize: 65536, PageSize: 256
 TimSize 0x1034
 FlashManager_Init:Version= 30400
 Search BBT in 0x0
 FlashManager_Init done
```



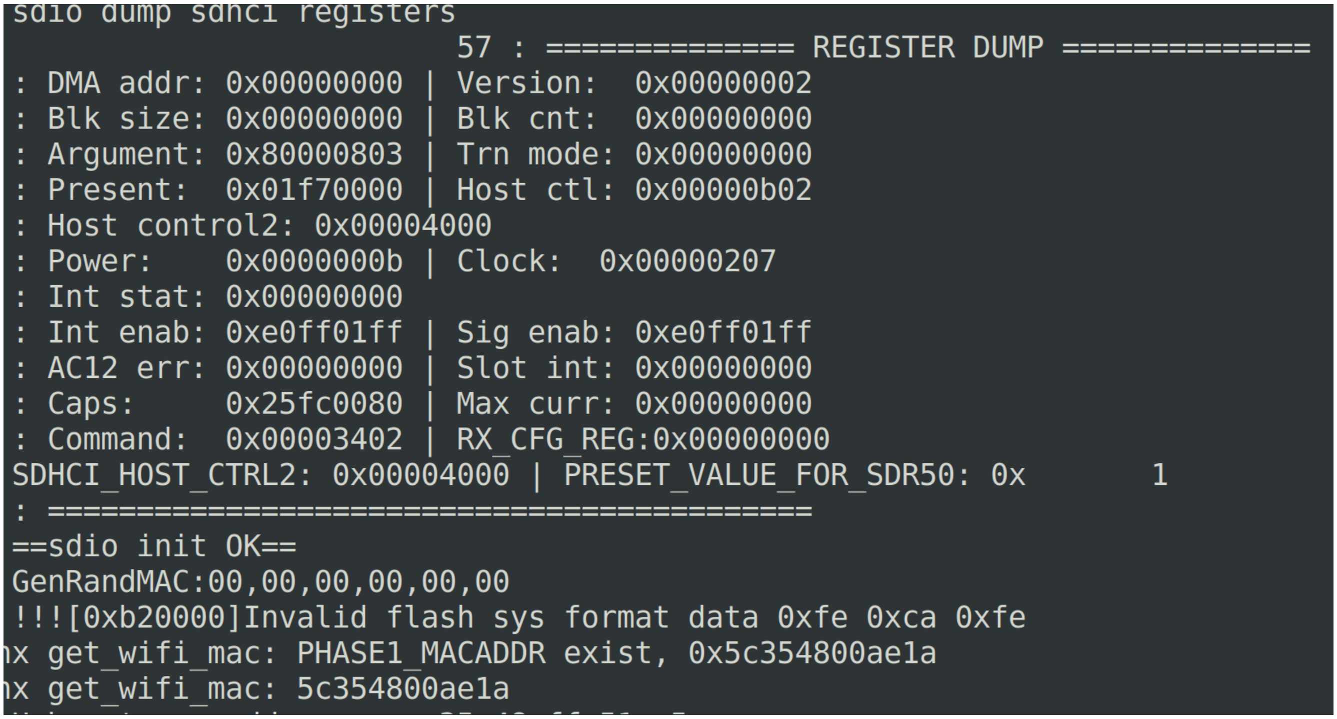
```
 psm header size:0x20, buffer addr:0x79a0000
 flash addr:0xad0000
 flash addr:0xad0000, ddr addr:0x7098ee0
                                        1f magic num:0x5a5a5a5a,0xffffffff
 flash addr:0xae0000
 flash addr:0xae0000, ddr addr:0x7098f40
                                        21 blk_num:1,len:0x0
 flash addr:0xaf0000
 flash addr:0xaf0000, ddr addr:0x7098fa0
                                        23 blk_num:2,len:0x0
 flash addr:0xb00000
 flash addr:0xb00000, ddr addr:0x7099000
                                        24 blk_num:3,len:0x0
 flash addr:0xb10000
 flash addr:0xb10000, ddr addr:0x7099060
                                        26 blk_num:4,len:0x31a2
```



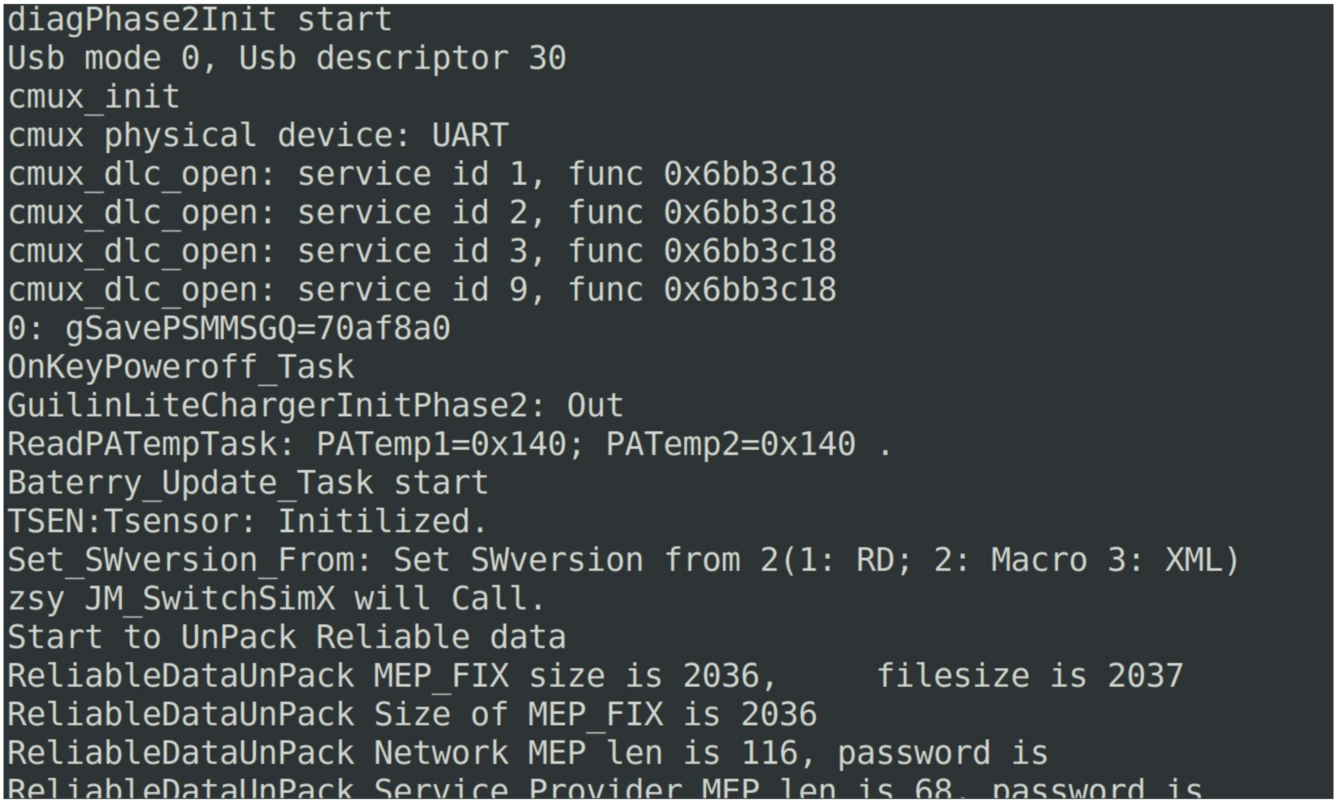
```
                   27 psm_block_init, file_num is 0,blk1 is 4
sm_block_init psm_fdi_info[0] is 4
sm_block_init, file_num is 1,blk1 is 1
sm_block_init psm_fdi_info[1] is 1
sm_block_init, file_num is 2,blk1 is 2
sm_block_init psm_fdi_info[2] is 2
sm_block_init, file_num is 3,blk1 is 3
sm_block_init psm_fdi_info[3] is 3
M_ExitProdMode,,,flash_layout->FBFStartAddress=b60000
M_ExitProdMode++Header=0x54524657,current Prod_Flag=0
DI_fclose_psm start, fileid:1
                             30 FDI_fclose_psm: done
MIC_GuilinLite_Configure_Marvell_LMIFI_V5R0 Enter.
IB_MMC1_IO_REG 0x81

MIC_GuilinLite_Configure_Marvell_LMIFI_V5R0 Exit.
P Initialize
ro_efuse = 145
ew profile num = 1
LCN_SVC_FP[0] = 0x15
LCN_SVC_FP[1] = 0x18
TC_Phase2_Init:
```



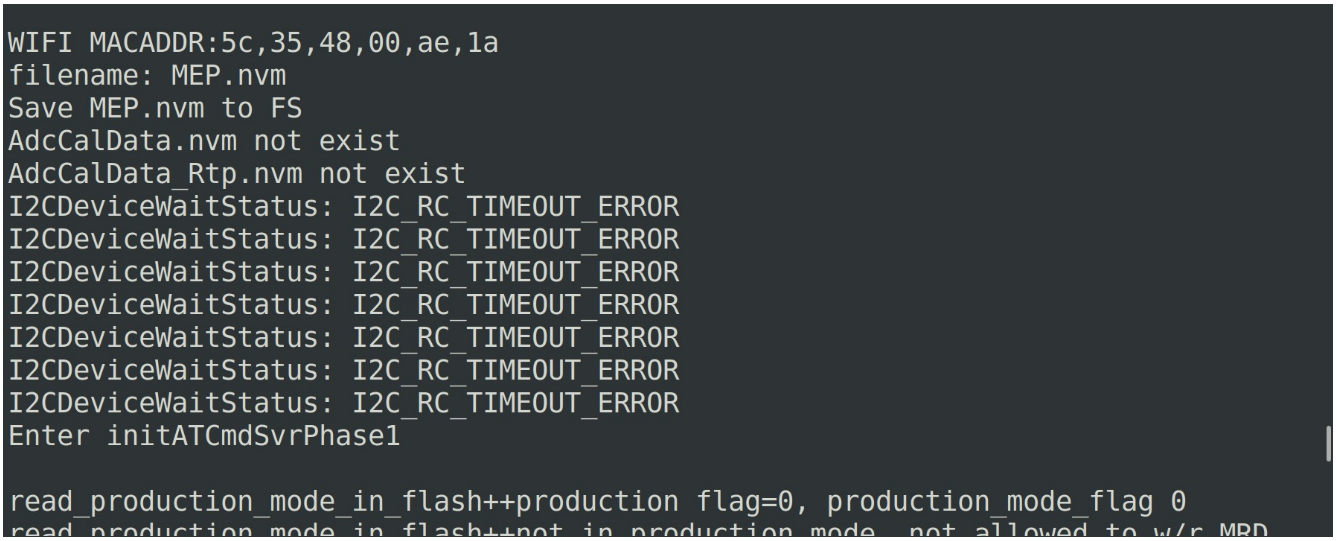
```
Recorded 2024- 3-7
Recorded 17,54,25
Recorded 0,RTC=0x0
InnerRTCTimeSet: newTime 1709834065
InnerRTCTimeSet: 2024/3/7 17:54:25
eeHandlerPhase2Init
==sdio init==
SDIO:Base 0xD4280800
zsy Platform_sdio_config_pin--board_type is 0x80
zsy sdio_config_falcon_5803_mifi_pin
zsy check_if_DCS_mode() != 1
HERON WIFI: read APB_spare5_reg 0xd4090110 is 0x18702f
HERON WIFI: read PMU_VRCR_reg 0xd4050018 is 0x1
HERON WIFI: read vcxo_req_mfpr 0xd401e0d4 is 0xb0c0
HERON WIFI: read clk_req_mfpr 0xd401e0cc is 0xc0c1
SDIO:SD0_HOST_PMU_AXI_CLOCK=119,SD1_HOST_PMU_AXI_CLOCK=112
SDIO:SD_HOST_CTRL_offset=b00

SDIO:SDHCI_TX_CFG=0x403700c5
SDIO:SD_CLOCK_CTRL_offset=4047
SDIO:SDHCI_CAPABILITIES1=0x80
SDIO:SDHCI_CAPABILITIES2=0x25fc
SDIO:SDHCI_CAPABILITIES3=0x2f77
```



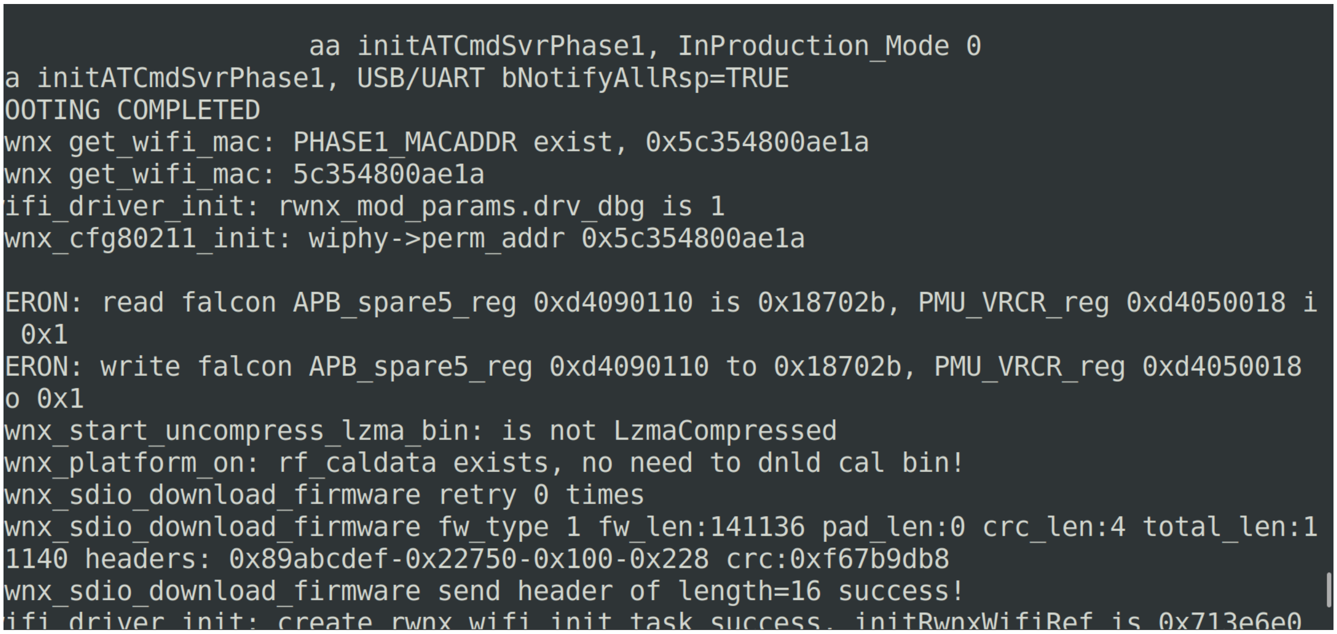
```
sdio dump sdhci registers
                         57 : ============== REGISTER DUMP ==============
: DMA addr: 0x00000000 | Version:  0x00000002
: Blk size: 0x00000000 | Blk cnt:  0x00000000
: Argument: 0x80000803 | Trn mode: 0x00000000
: Present:  0x01f70000 | Host ctl: 0x00000b02
: Host control2: 0x00004000
: Power:    0x0000000b | Clock:  0x00000207
: Int stat: 0x00000000
: Int enab: 0xe0ff01ff | Sig enab: 0xe0ff01ff
: AC12 err: 0x00000000 | Slot int: 0x00000000
: Caps:     0x25fc0080 | Max curr: 0x00000000
: Command:  0x00003402 | RX_CFG_REG:0x00000000
SDHCI_HOST_CTRL2: 0x00004000 | PRESET_VALUE_FOR_SDR50: 0x       1
: ===========================================
==sdio init OK==
GenRandMAC:00,00,00,00,00,00
!!![0xb20000]Invalid flash sys format data 0xfe 0xca 0xfe
nx get_wifi_mac: PHASE1_MACADDR exist, 0x5c354800ae1a
nx get_wifi_mac: 5c354800ae1a
```



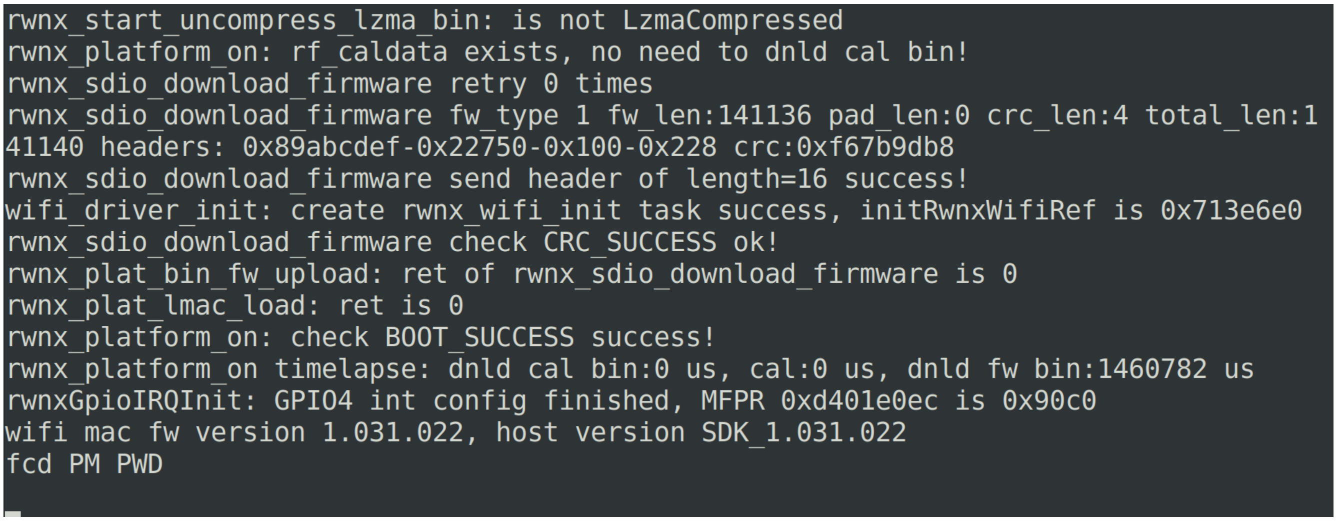
```
diagPhase2Init start
Usb mode 0, Usb descriptor 30
cmux_init
cmux physical device: UART
cmux_dlc_open: service id 1, func 0x6bb3c18
cmux_dlc_open: service id 2, func 0x6bb3c18
cmux_dlc_open: service id 3, func 0x6bb3c18
cmux_dlc_open: service id 9, func 0x6bb3c18
0: gSavePSMMSGQ=70af8a0
OnKeyPoweroff_Task
GuilinLiteChargerInitPhase2: Out
ReadPATempTask: PATemp1=0x140; PATemp2=0x140 .
Baterry_Update_Task start
TSEN:Tsensor: Initilized.
Set_SWversion_From: Set SWversion from 2(1: RD; 2: Macro 3: XML)
zsy JM_SwitchSimX will Call.
Start to UnPack Reliable data
ReliableDataUnPack MEP_FIX size is 2036,     filesize is 2037
ReliableDataUnPack Size of MEP_FIX is 2036
ReliableDataUnPack Network MEP len is 116, password is
ReliableDataUnPack Service Provider MEP len is 68, password is
```



```
WIFI MACADDR:5c,35,48,00,ae,1a
filename: MEP.nvm
Save MEP.nvm to FS
AdcCalData.nvm not exist
AdcCalData_Rtp.nvm not exist
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
I2CDeviceWaitStatus: I2C_RC_TIMEOUT_ERROR
Enter initATCmdSvrPhase1

read_production_mode_in_flash++production flag=0, production_mode_flag 0
read_production_mode_in_flash++not in production mode, not allowed to w/r MRD
```



```
                   aa initATCmdSvrPhase1, InProduction_Mode 0
a initATCmdSvrPhase1, USB/UART bNotifyAllRsp=TRUE
OOTING COMPLETED
wnx get_wifi_mac: PHASE1_MACADDR exist, 0x5c354800ae1a
wnx get_wifi_mac: 5c354800ae1a
ifi_driver_init: rwnx_mod_params.drv_dbg is 1
wnx_cfg80211_init: wiphy->perm_addr 0x5c354800ae1a

ERON: read falcon APB_spare5_reg 0xd4090110 is 0x18702b, PMU_VRCR_reg 0xd4050018 i
 0x1
ERON: write falcon APB_spare5_reg 0xd4090110 to 0x18702b, PMU_VRCR_reg 0xd4050018
o 0x1
wnx_start_uncompress_lzma_bin: is not LzmaCompressed
wnx_platform_on: rf_caldata exists, no need to dnld cal bin!
wnx_sdio_download_firmware retry 0 times
wnx_sdio_download_firmware fw_type 1 fw_len:141136 pad_len:0 crc_len:4 total_len:1
1140 headers: 0x89abcdef-0x22750-0x100-0x228 crc:0xf67b9db8
wnx_sdio_download_firmware send header of length=16 success!
ifi_driver_init: create rwnx_wifi_init_task success, initRwnxWifiRef is 0x713e6e0
```



```
rwnx_start_uncompress_lzma_bin: is not LzmaCompressed
rwnx_platform_on: rf_caldata exists, no need to dnld cal bin!
rwnx_sdio_download_firmware retry 0 times
rwnx_sdio_download_firmware fw_type 1 fw_len:141136 pad_len:0 crc_len:4 total_len:1
41140 headers: 0x89abcdef-0x22750-0x100-0x228 crc:0xf67b9db8
rwnx_sdio_download_firmware send header of length=16 success!
wifi_driver_init: create rwnx_wifi_init task success, initRwnxWifiRef is 0x713e6e0
rwnx_sdio_download_firmware check CRC_SUCCESS ok!
rwnx_plat_bin_fw_upload: ret of rwnx_sdio_download_firmware is 0
rwnx_plat_lmac_load: ret is 0
rwnx_platform_on: check BOOT_SUCCESS success!
rwnx_platform_on timelapse: dnld cal bin:0 us, cal:0 us, dnld fw bin:1460782 us
rwnxGpioIRQInit: GPIO4 int config finished, MFPR 0xd401e0ec is 0x90c0
wifi mac fw version 1.031.022, host version SDK_1.031.022
fcd PM PWD
```

Note : The firmware version is available in the image above.

############### End of Document ##################