Msft.guy@googlewave.com: Jun 29

iBSS payload: 3.1.2 3GS

Only works with 3GS iBSS 636.66 (3.1.2)
Use if you have saved SHSH for 3.1.2 FW.

```
    xpwntool ~/Desktop/iPhone2,1_3.1.2_7D11_Restore/Firmware/dfu/iBSS.n88ap.RELEASE.dfu iBSS.dec -iv 41639d34547ae3dd7921bf3539dba529 -k
    9121de4a038675d92e1a28683b2138b7a3bdb80994273d090398051c7f5af53c

    shasum iBSS.dec

    dd if=iBSS.dec of=ib_8kchunk bs=$[0x2000] count=1

    shasum ib_8kchunk

    printf "\x00\x20\x00\x41" > irqaddr

    shasum irqaddr

    dd if=irqaddr of=ib_8kchunk bs=1 count=4 seek=$[0x38] conv=notrunc

    shasum ib_8kchunk

    arm-elf-gcc -Ttext=0x41002000 -Wl,-e,_main ibss_pwn.c -o payload.elf -nostdlib -mthumb-interwork

    arm-elf-objcopy -O binary payload.elf ibss_payload.bin

    shasum ibss_payload.bin

    rm payload.elf

    cp ib_8kchunk exploit

    cat ibss_payload.bin >> exploit

    shasum exploit
```

and output:

```
    img3.c:createAbstractFileFromImg3:646: 4527cc9eaceaa0fffc806ce01b2e0bd66838e9d5633f9c75adc16afa55d2ff2c96a4f0eb0cc6596ff8f01566a0436f62
    3cc14114117ea699f778cfc66083ffa10eded9d3  iBSS.dec
    1+0 records in
    1+0 records out
    8192 bytes transferred in 0.000058 secs (141398100 bytes/sec)
    3fa7e959e1c11b0a6781f15da93f2224907bb736  ib_8kchunk
    e8959d375f1b34252ff2bef36abde432d0d09f5d  irqaddr
    4+0 records in
    4+0 records out
    4 bytes transferred in 0.000041 secs (97542 bytes/sec)
    86a1d085da0a864c9c3a155650899a3f2804d8c3  ib_8kchunk
    b742ae5203c2483d25f1f5b89746f9b4117f3cc1  ibss_payload.bin
    40f688edc676c7c7cc7adb0528eddcb5a75ca31a  exploit
```

Zip File

ibss_payload.zip

Msft.guy@googlewave.com: Use Jun 29

```
iRecovery -k exploit
```

to send this to the iBSS.
Only works with 3GS iBSS 636.66

Tags: +   Images   Next wave