Msft.guy@googlewave.com: Jun 12

iPhone 3GS 3.1.2 iBoot pwn payload + instructions

Only works with 3GS iBoot 636.66 (3.1.2)

iboot_payload.zip

```
# if not 94095e432ef5b967ef1460d95bb75473a65bfb5f, you've done something wrong
shasum iboot_payload.bin

xpwntool CHANGE_ME/iPhone2,1_3.1.2_7D11_Restore/Firmware/all_flash/all_flash.n88ap.production/iBoot.n88ap.RELEASE.img3 iBoot.dec -iv 127aa60e77da219961ee70707f44cbd4 -k
c72ab4aae971f3a9ec356dfe555e4aef72d8e96c480698445ac236904e6a3443

# if not f9ad80838300a0f5ebbb686b0f24d61aece318ea, you've done something wrong
shasum iBoot.dec

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

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

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

# if not 04b28f2c1e438fcc2423f08fe260834fd97d11e3, you've done something wrong
shasum ib_8kchunk

cp ib_8kchunk exploit

cat iboot_payload.bin >> exploit

# if not 6bef8713ae86838740f4fa081e4d38563bcb077c, you've done something wrong
shasum exploit
```

Msft.guy@googlewave.com: Use Jul 28

itunnel_mux_r61.exe --exploit exploit

OR

iRecovery -k exploit

to send this to the iBoot.

Only works with 3GS iBoot 636.66

Kalyanspb@googlewave.com: Sorry, I'm a newbie both in "pwning" and "waving", so I didn't manage to get the clear instructions from the "Slow Discussion". It may be also useful to know that I'm using WinXP. Jun 13

Msft.guy@googlewave.com: So, what is your question? Jun 14

Kalyanspb@googlewave.com: 1. Could you, please, give simplier step-by-step instruction? Jun 14

(though I don't understand the first step: # if not 94095e432ef5b967ef1460d95bb75473a65bfb5f, you've done something wrong shasum iboot_payload.bin)

2. Or if you have not enough time for such explanations, could you, please, give me a link, which would explain the matter for a newbie?

Msft.guy@googlewave.com: 1. Those are the commands required to build the iBoot exploit given the (attached) payload file. You can paste those into a shell script or copy to console and execute manually. Jun 15

2. man 1 shasum http://linux.die.net/man/1/shasum

xpwntool is an utility from the xpwn package that decrypts img3 files.

dd, printf, cp, cat - Unix commands, see man pages for details.

- comment in Unix shell scrpts; I addedd shasum hashes for most intermediate files to help people troubleshoot the process.

Peacepot@googlewave.com: hi msft guy, desperately need help here..iphone 2g 8gb running OS 3.0 jb using redsn0w (if i remember correctly), Jun 19

And now it cannot boot,only apple logo and after that it'll auto shut off,and if i power it up again - it repeats.

It begans after a fail update of facebook..and before that problem solved, i regretly played with categories (from cydia) and when it respring this madness begin..

have spent 9hrs (or more),and im kinda tired so i must take a rest,but first i needed to ask:

i successfully tried irecovery (setenv,saveenv,fsboot,reboot,iBoot-596.24), but the problem still there,

now i already dl-ed recoveryramdiskbuilder_rev_2.zip, and im ready to try ur methods,

but since im not 3.1.2, i dont know which "pwned .ipsw" file i need..(the dmg and kernelcache)

i googled "7D11 restore ramdisk "2G" for 3.0 2G" and havent saw any good links..

should i use the ipsw when i jb my iphone? (i even already forgot wheres the file,i think it was iphone1,1_3.0_7A341_Restore.ipsw?)

well infact i dont know where should i download, with all the 'custom restore','custom firmware' naming..

thats why im still happy with 3.0..really sorry if i missed any comments about this,already tried reading all the comments b4 i decide to ask u.

thx for ur reply, i desperately need to get my data :(

Peacepot@googlewave.com: UPDATE... Jun 21

well at least now i can breath easy since i already grab my files, but i still having problem with the iphone loading up normally, i think i'll let it be until i found any solution.

Thanks msft.guy for your methods, still waiting for ur comments here, or any helps to get my phone load normally again :)

Msft.guy@googlewave.com: If you copied the data (disk image or managed to mount mnt2) then just restore the phone. You should be able to restore to custom FW if you need unlock, or just DFU-restore if you only need JB.. Jun 21

Peacepot@googlewave.com: THX for replying, i thought this wave is dead... well i managed to download it,and extract the files without any errors, but i cannot mount it since there was a 'sibling link' error. should i upload it to the phone? i mean so it can return to it previous state (with upgraded fw?).. if i just do a restore then the file jwill be gone right? thx... Jun 22

Msft.guy@googlewave.com: Peacepot: what exactly did you download and how did you extract the files if it cannot be mounted? .. Jun 22

Peacepot@googlewave.com: hi msft, i can mount disk0s1, but theres no disk0s2s1 (bcause iphone 2G perhaps), so after reading mr.bassisst problem, i download disk0s2 (8GB whew) and yeah it contains all the data. Jun 22
i dont know whats wrong, i just use mnt_hfs and it cant be mount, just like in your video (i dont even quite understand 'mount', my console background is DOS), and when i fsck it it says invalid siblink link.. as you can see below i already tried using -r to fix it but no luck..

Peacepot@googlewave.com: hm about the extract thing, well just like u said, i rename it to disk0s2.dmg, but before using diskwarior,recovermac etc, i just try to view it using transmac (windows trial 15 days only :( ), it went well.. Jun 22

Peacepot@googlewave.com: ok while waiting for any reply (PLSSSSSS) Jun 19
im back at reading and found that it doesnt matter what my FW before, right?
currently im still downloading iPhone1_1_3.1.2_7D11_Custom_Restore_Activated, is this correct?

Peacepot@googlewave.com: Ok i've tried it and i already go wayyyy to the kill 1... Jun 20
but now it's still restarting.. argh, what should i do??

Peacepot@googlewave.com: Now im able to view the mnt1/ folders, but no luck with mnt2/, its the one with our files in it right? i think i have the same problem with mr.bassist in the 'slow discussion wave 1', i dont see any disk0s2s1, there's disk0s2 only, and when i fsck it failed... currently im downloading it... Jun 21
Any help here guys? please?

Peacepot@googlewave.com: ok got the files, but iphone still on loop... already try fsck_hsf /dev/disk0s2, and it said Invalid Sibling Link. Jun 21
Googled it and found that people can repair it using fsck_hsf -r, but that didn't work for me (perhaps bcause the space is run out?), it said The volume Data could not be repaired.....
Wondering if there is any way to bypass the loop...

Kcolyhs@googlewave.com: Will this method work with a 3GS, 3.1.2, new bootrom, jailbroken with Blackra1n. All SHSH's available and on file. But phone is in "DFU brick" mode? Jun 29

Msft.guy@googlewave.com: Well, if it's in DFU you need an iBSS payload.. and personalized iBSS (iTunes will upload that at the very beginning of the restore process, be sure to disconnect USB once you get a white screen). Jun 29

Kcolyhs@googlewave.com: I am able to get to white screen, and follow the instructions loading " irec -k /iPhone2,1_3.1.2_7D11_Restore/basechunk" from the 312ibec payload you provided, but the next steps nothing loads. Do I have to modify the basechunk file? Jun 29

Msft.guy@googlewave.com: i'm not sure what exactly this basechunk is, and how you got 312 ibec to load.. Jun 29

Kcolyhs@googlewave.com: So the first step after white screen is loading modified "ibss_payload.bin"?, how do i modify it? Jun 29
The basechunk is the 312ibec payload you provided. i don't know if it actually loads or not.

Msft.guy@googlewave.com: The white screen you're referring to is most likely iBSS. you can check that using iRecovery -s console output. Jun 29

Kcolyhs@googlewave.com: iRecovery - Recovery Utility for 0x1281 and WTF. Jun 29
by wEsTbAeR-- and Tom3q

Got USB

```
=======================================
::
:: iBSS for n88ap, Copyright 2009, Apple Inc.
::
::    BUILD_TAG: iBoot-636.66
::
::    BUILD_STYLE: RELEASE
::
::    USB_SERIAL_NUMBER: CPID:8920 CPRV:15 CPFM:03 SCEP:03 BDID:00 ECID:000000183A06238D IBFL:00 SRNM:[87942GEP3NR]
::
=======================================

Entering recovery mode, starting command prompt
limiting USB input current to 100 mA
(Recovery) iPhone$
```

That is my console output when first connecting

Msft.guy@googlewave.com: Here's the iBSS payload w/ instructions Jun 29
iBSS payload: 3.1.2 3GS
are you getting the same hashes as in the provided instructions?

Kcolyhs@googlewave.com: Thank you very much for your help Jun 29

Kcolyhs@googlewave.com: I will try what you suggested and post back later. Thanks again. Jun 29

Kcolyhs@googlewave.com: I have a problem when executing: "arm-elf-gcc -Ttext=0x41002000 -Wl,-e,_main ibss_pwn.c -o payload.elf -nostdlib -mthumb-interwork" Jul 1
I get the error: "-bash: arm-elf-gcc: command not found"
All previous steps work, and hashes are correct. I am using an intel mac 10.6.3, I have the latest xcode and x11 installed. I downloaded Macports, and installed the arm-elf-gcc ports through terminal, but still get the same error. I would appreciate any guidance on how to proceed.

Msft.guy@googlewave.com: You don't need to build the code chunk if you download the zip file from the wave; only assemble (xpwntool and dd commands). If hash of **exploit** file matches then you can proceed with using irecovery -k exploit command and then -regular ramdisk steps. Jul 1

Kcolyhs@googlewave.com: So i only need to enter the first 2 lines: 1) xpwntool then 2) dd then what do i do the checksums are correct. What about the last 2 lines: cp ib_8kchunk exploit, and cat ibss_payload.bin >> exploit do i use them? Jul 1
I am sorry if this is a dumb question, but having downloaded the ibss_payload file from the wave, is it passively accessed by xpwntool, or do I use it in the above lines?

Msft.guy@googlewave.com: It is, in fact, kind of a dumb question. Jul 1
>> If hash of **exploit** file matches then you can proceed
Do you have an 'exploit' file with the same hash as in the wave? If not, then maybe you need to run those commands? What's so difficult about that?

Kcolyhs@googlewave.com: Ok, I have got the exploit with the correct hash. Jul 2
So I now go to the iRecovery -s window, and type: "iRecovery -k exploit"?
I did that but the white screen remains unchanged.

I then entered the following lines one by one:

- iRecovery -f 018-6051-014.ssh.dmg
- iRecovery -c ramdisk 0x90000000
- iRecovery -f kernelcache.release.s5l8920x
- iRecovery -c bootx

The white screen does not change, is that expected?

I then started Cyberduck, but itnl_rev5 gives a "Permission denied" message.
What do I need to get itnl_rev5 to work?
In Cyberduck: server=localhost, port=2022, user=root, password=alpine is that correct?

Kcolyhs@googlewave.com: The above 4 iRecovery commands are entered. The dmg.ssh loads, the ramdisk does nothing, the kernelcache loads, the bootx does nothing. Jul 4
I remain at the white screen throughout.
Tunneling gives the message: "waiting for device", Cyberduck does not connect.
If I enter "iRecovery -s" at this stage I get the following:

```
 /DFU\ Recover\ Project\ Step_OK/iRecovery -s
iRecovery - Recovery Utility for 0x1281 and WTF.
by wEsTbAeR-- and Tom3q

Got USB
Error -9 when setting configuration
Error -16 when claiming interface
Error -536870195 when setting altinterface
```

So where is the problem?
My "exploit" has the correct hash. Am I using the -k exploit correctly?
When do I use: iRecovery -k exploit? At the first terminal window, before connecting the iPhone?, or after the iRecovery -s white screen stage?

Remember I have a 3GS, new bootrom, blackra1n jailbreak, and in "PERMANENT-DFU-BRICK" mode.

I have photos that I need to recover, and that is my prime interest.

Thanks

Kcolyhs@googlewave.com: Ok, I got the process to work and am now connected by Cyberduck. Jul 4
It was the damned iRecovery version that would not accept the -k command, that is why the whole stupid process failed over and over.
I downloaded several versions, until I found one that works.
However, the one that accepts the -k command, does not show any progress while executing the -f, or -c commands, so basically you hope and pray that it is working!.
I think when writing up this process we should have been warned about compatibility issues with different versions of the tools used.

Andrei.d.bel@googlewave.com: Hm.... Jul 4

Mikey351@googlewave.com: I have the a 3GS that was running the tethered Blackra1n JB for 3.1.2 and new bootrom. I have followed all the instructions in msft.guy's post at the begining of the wave and all my sh checksums match, so no problem there. I downloaded the iRecovery for Win32 using the link supplied by msft.guy too, and it is with iRecovery I am having a problem. Jul 12
When I run iRecovery -k exploit, this is what I get back:

```
C:\irecovery-0.3.2-win32>irecovery -k exploit
iRecovery - Recovery Utility
by westbaer
Thanks to pod2g, tom3q, planetbeing, geohot and posixninja.

Found iPhone/iPod in Recovery mode
usbhax 0x21-2-0-0: fffff8c
Closing USB connection...
```

Not sure if this is what I should see, because when I do the next command, i get back:

```
C:\irecovery-0.3.2-win32>irecovery -f 018-6051-014.dmg.ssh
iRecovery - Recovery Utility
by westbaer
Thanks to pod2g, tom3q, planetbeing, geohot and posixninja.

No iPhone/iPod found.
```

I have tried disconnecting the iphone and then plugging it back in however I still get the No iPhone/iPod found, and I also get the "USB device not recognised" error from Windows too.

Have I got the steps wrong? I thought, because I have the new bootrom 3GS that the steps would be in the following order.

1. Create files as list above
2. iRecovery -k exploit
3. then following instructions on the main page from the main section under the heading *Put your phone in recovery mode

Not sure where I went wrong. Any help appreciated.

Mike
PS. I do not have any SHSHs for my 3.1.2

Msft.guy@googlewave.com: Do you have 312 shsh ? Do you have TeamViewer installed? it's a free DL. Jul 12
After you install it, email id/pass to msft.guy@gmail.com, I'll see

Mikey351@googlewave.com: thanks! downloading it now :) Jul 12

Mikey351@googlewave.com: damn, the battery has gone flat, downloaded and installed teamviewer though, seems good now if only the ipod would hurry up and charge. Jul 12

what I can do ;)

Mikey351@googlewave.com: No, where can i get it? Jul 12

Mikey351@googlewave.com: no, sorry, no shsh Jul 12

Mikey351@googlewave.com: ok, installed and email sent :) Jul 12

Msft.guy@googlewave.com: 15 min, sry Jul 12

Mikey351@googlewave.com: thats cool. thanks. Jul 12

Nguyenbakim@googlewave.com: Hi, Mike, have you fixed your iPhone, I have the same situation like yours, after "irecovery -k exploit" the iPhone stop respond to irecovery, and i am stucked Jul 28

Mikey351@googlewave.com: unfortunately no. Thanks to msft.guy's help i was able to get in and back up what i needed, however after running fsck, rebooting and trying to jailbreak again with blackra1n it still got stuck on geohots picture. Aug 3

Tags: +

Images | Next unread 41