Don't Forget - 1/8/2017 - Jon Sawyer -jcase@cunninglogic.com

DJI don't forget about what happens when you defraud the open source community by refusing to abide by the licenses. You are using code I helped write in your products, at the same time refusing to honor the licenses of the open source projects you are using.

With that rant said, don't forget about jcase. Isn't it fantastic when you piss off those that hack embedded devices for a living? Hell you base your system on Android 4.x, that was like my heyday of hacking. Suckers.

One of the best tactics when repeatedly targeting the same device, is to keep pressing the same class of vulnerability, or keep targeting the same set of code until that bit of code is exhausted of vulnerabilities. Save your other bugs.

So here is the vulnerable code:

```
MOV.W           R9, #0
MOV.W           R10, #1
ADD.W           R11, SP, #0x220+var_1D4
LDRH.W          R1, [R4,#0x202]
STR.W           R9, [SP,#0x220+var_220]
STR.W           R11, [SP,#0x220+var_21C]
STR.W           R10, [SP,#0x220+var_218]
STR.W           R10, [SP,#0x220+var_214]
MOV             R2, R9
MOV             R3, R10
LDR.W           R0, [R4,#0x1C0]
BL              sub_1A0EC
LDR.W           R3, [R11]
MOVS            R0, #2
MOVS            R1, #7
LDRH.W          R2, [R4,#0x202]
STR             R3, [SP,#0x220+var_220]
STR             R1, [SP,#0x220+var_214]
STR             R0, [SP,#0x220+var_21C]
STR.W           R10, [SP,#0x220+var_218]
STR.W           R10, [SP,#0x220+var_210]
LDR.W           R0, [R4,#0x1C0]
MOV             R1, R9
MOV             R3, R9
BL              sub_19E88
BL              sub_18C9C
BL              sub_18CFC
LDR.W           R3, =(aDataFtpUpgrade - 0x2062E)
LDR.W           R2, =(aDataFtpUpgra_0 - 0x20636)
ADD             R3, PC  ; "/data/ftp/upgrade/upgrade/signimgs/"
STR             R3, [SP,#0x220+var_21C]
LDR.W           R3, =(aBusyboxTarXfSC - 0x20640)
ADD             R2, PC  ; "/data/ftp/upgrade/dji_system.bin"
STR             R2, [SP,#0x220+var_220]
MOV             R1, R9
MOV.W           R2, #0x100
ADD             R3, PC  ; "busybox tar -xf %s -C %s"
ADD             R0, SP, #0x220+command
BLX             __sprintf_chk
LDR.W           R0, =(aDjiDumlServi_4 - 0x20650)
LDR.W           R1, =(aSys_up_sec_up_ - 0x20652)
ADD             R0, PC  ; "dji/duml/service/system/src/sys_p1.c"
ADD             R1, PC  ; "sys_up_sec_up_thread"
MOVW            R2, #0x5A2
STR             R0, [SP,#0x220+var_220]
STR             R1, [SP,#0x220+var_21C]
STR             R2, [SP,#0x220+var_218]
MOVS            R0, #0x63
MOVS            R1, #3
ADD             R2, SP, #0x220+var_1AC
MOVS            R3, #0x80
BLX             duss_log_gen_head
CBZ             R0, loc_20678
```

Don’t see it? Don’t worry its kinda hard to spot, super hard if you don’t know the DJI update system.

dji_system.bin is a tar ball pushed over open ftp to /ftp/upgrade. /ftp is actually /data/ftp. had they used the /ftp paths, this bug would be worthless. They used /data/ftp ;p

We want to put a hardlink in a tar ball, pointing to something on /data we want to overwrite, like the ‘anti rollback’ protection file. Had they used the /ftp path, it would have been “cross device” and we wouldn’t be able to use a hard link to write the ‘anti rollback’ file. Tsk tsk DJI.

So, first busybox (or the tar format? idk) won’t allow a hardlink to be extracted unless the target is also in the tar file. Busybox also removes prefixed ‘/‘ from paths, but NOT from link targets :)

So we craft a custom tar file. This was the biggest challenge, my checksum code was so bad when make these

contents:
dont_forget_about_jcase - 100mb dummy file for some delay before dji_sys deletes it all
/data/upgrad/backup/wm220.cfg.sig - 0byte file, we just need it in the tar before the hardline
jcase - hardlink to /data/upgrad/backup/wm220.cfg.sig

When we extract this, it is extracted to /data/ftp/upgrade/upgrade/signimags, and the tar contacted /data/* files have the ‘/‘ prefixed removed. The jcase ‘file gets hardlinked to the real wm220.cfg.sig.

Wait hardlink? What is that? It is kinda like a shortcut/symlink but not really. It actually creates another ‘file’ that actually points to the same contents of the original. So if you change one, the both change! Neat!

Ok so once jcase is on disk, what do we do? We use ftp to write to overtop of the hardlink! This will change the contents of the original file! We write a 0 byte file to jcase, which makes the real wm220.cfg.sig file 0 bytes!

Boom you can downgrade.

Cheers!

Shout outs!

beaups, diff, rotlogix, and everyone at dji-rev. Thank you all for helping me through my drone hacking journey!