

tenda overflow vulnerability

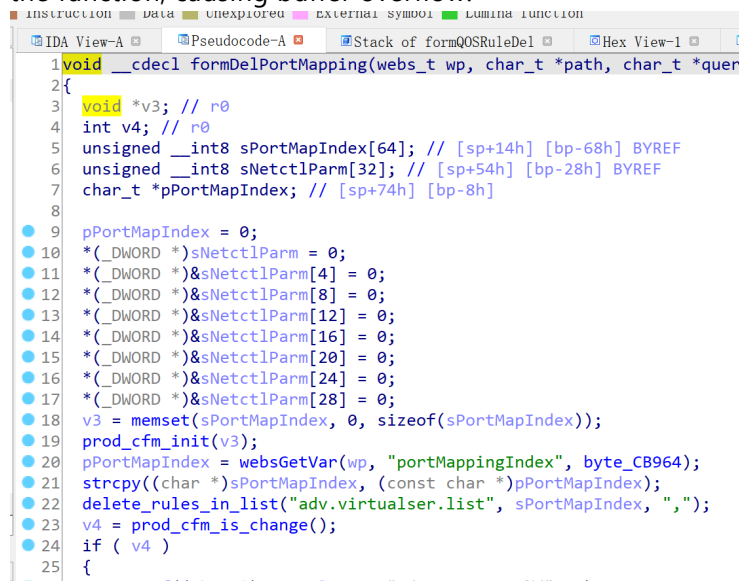
vendor:Tenda
product:G1,G3
version:V15.11.0.17(9502)_CN(G1),
V15.11.0.17(9502)_CN(G3)
type:Buffer Overflow
author:Jinwen Zhou、Yifeng Li、Yongjie Zheng;
institution:potatso@scnu、feng@scnu、eifiz@scnu

Vulnerability description

We found a buffer overflow vulnerability in Tenda Technology Tenda's **G1 and G3** routers with firmware which was released recently, allows remote attackers to execute arbitrary code from a crafted GET request.

Buffer Overflow vulnerability

In **formDelPortMapping** function, the parameter **"portMappingIndex"** is directly **strcpy** to a local variable placed on the stack, which overrides the return address of the function, causing buffer overflow.



```
1 void __cdecl formDelPortMapping(webs_t wp, char_t *path, char_t *quer
2 {
3     void *v3; // r0
4     int v4; // r0
5     unsigned __int8 sPortMapIndex[64]; // [sp+14h] [bp-68h] BYREF
6     unsigned __int8 sNetctlParm[32]; // [sp+54h] [bp-28h] BYREF
7     char_t *pPortMapIndex; // [sp+74h] [bp-8h]
8
9     pPortMapIndex = 0;
10    *(_DWORD *)sNetctlParm = 0;
11    *(_DWORD *)&sNetctlParm[4] = 0;
12    *(_DWORD *)&sNetctlParm[8] = 0;
13    *(_DWORD *)&sNetctlParm[12] = 0;
14    *(_DWORD *)&sNetctlParm[16] = 0;
15    *(_DWORD *)&sNetctlParm[20] = 0;
16    *(_DWORD *)&sNetctlParm[24] = 0;
17    *(_DWORD *)&sNetctlParm[28] = 0;
18    v3 = memset(sPortMapIndex, 0, sizeof(sPortMapIndex));
19    prod_cfm_init(v3);
20    pPortMapIndex = websGetVar(wp, "portMappingIndex", byte_CB964);
21    strcpy((char *)sPortMapIndex, (const char *)pPortMapIndex);
22    delete_rules_in_list("adv.virtualser.list", sPortMapIndex, ",");
23    v4 = prod_cfm_is_change();
24    if ( v4 )
25    {
```

PoC

Buffer Overflow

We set the value of **portMappingIndex** as **aaaaaaaaaaaaaaaaaaaaaaaa.....** and the router will cause buffer overflow.

