

# tenda overflow vulnerability

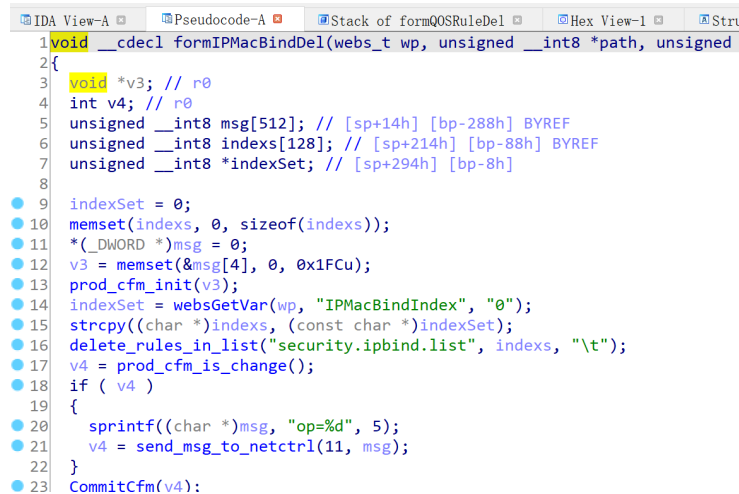
vendor:Tenda  
product:G1,G3  
version:V15.11.0.17(9502)\_CN(G1),  
V15.11.0.17(9502)\_CN(G3)  
type:Buffer Overflow  
author:Jinwen Zhou、 Yifeng Li、 Yongjie Zheng;  
institution:potatso@scnu、 feng@scnu、 eifiz@scnu

## 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 **formIPMacBindDel** function, the parameter **"IPMacBindIndex"** 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 formIPMacBindDel(webs_t wp, unsigned __int8 *path, unsigned
2 {
3     void *v3; // r0
4     int v4; // r0
5     unsigned __int8 msg[512]; // [sp+14h] [bp-288h] BYREF
6     unsigned __int8 indexs[128]; // [sp+214h] [bp-88h] BYREF
7     unsigned __int8 *indexSet; // [sp+294h] [bp-8h]
8
9     indexSet = 0;
10    memset(indexs, 0, sizeof(indexs));
11    *(_DWORD *)msg = 0;
12    v3 = memset(&msg[4], 0, 0x1FCu);
13    prod_cfm_init(v3);
14    indexSet = websGetVar(wp, "IPMacBindIndex", "0");
15    strcpy((char *)indexs, (const char *)indexSet);
16    delete_rules_in_list("security.ipbind.list", indexs, "\t");
17    v4 = prod_cfm_is_change();
18    if ( v4 )
19    {
20        sprintf((char *)msg, "op=%d", 5);
21        v4 = send_msg_to_netctrl(11, msg);
22    }
23    CommitCfm(v4);
```

## PoC

### Buffer Overflow

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



















