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