Tenda AC6V1.0 V15.03.05.19 Stack overflow vulnerability

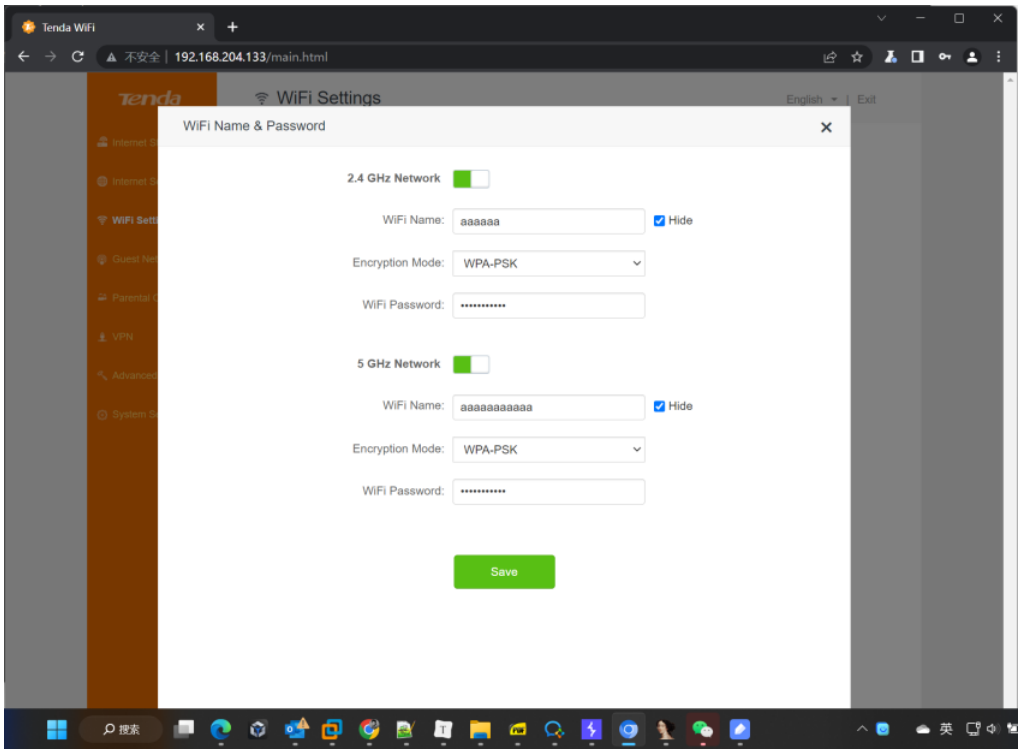
Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2681.html

Affected version

Vulnerability details

This vulnerability lies in the `/goform/WifiBasicSet` page, While processing the `security` parameters for a post request, the value is directly `strcpy` to a local variable placed on the stack, which overrides the return address of the function, causing buffer overflow. The details are shown below:

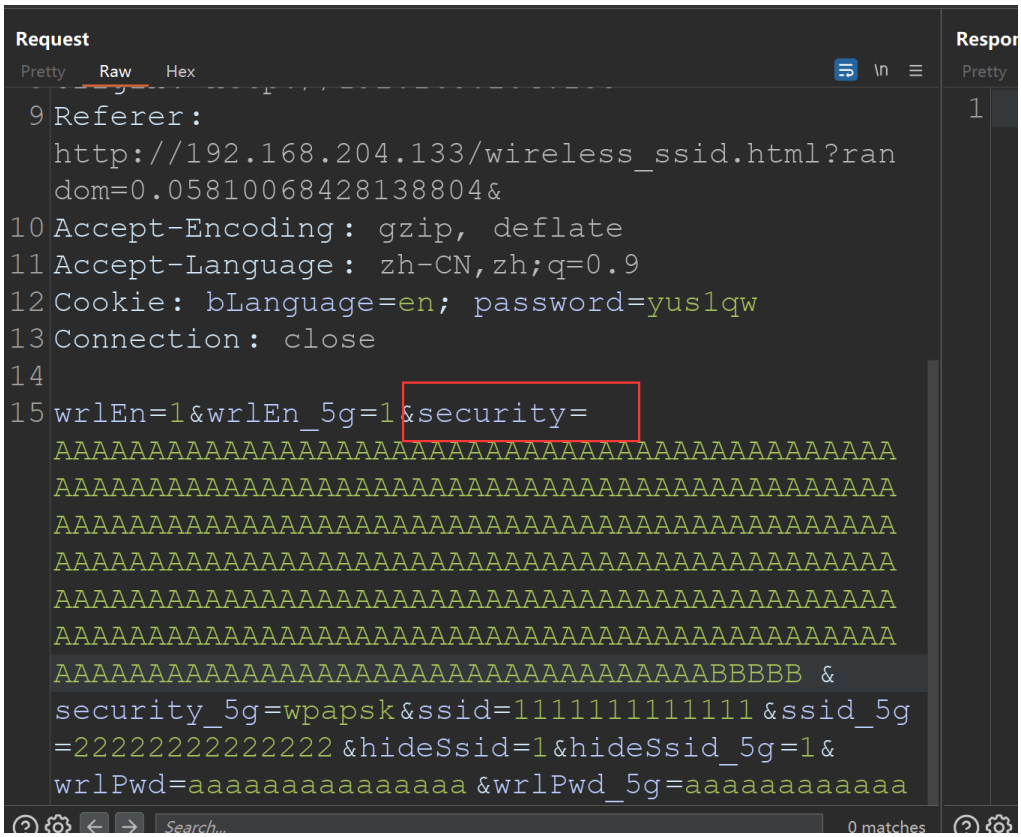



```
16  int Value; // r0
17  int uptime; // r0
18  int v16; // r0
19  int v17; // r0
20  char v20[32]; // [sp+1Ch] [bp-BB8h] BYREF
21  char v21[32]; // [sp+3Ch] [bp-B98h] BYREF
22  int v22[129]; // [sp+5Ch] [bp-B78h] BYREF
23  char v23[256]; // [sp+260h] [bp-974h] BYREF
24  char v24[256]; // [sp+360h] [bp-874h] BYREF
25  char v25[256]; // [sp+460h] [bp-774h] BYREF
26  char v26[256]; // [sp+560h] [bp-674h] BYREF
27  char v27[256]; // [sp+660h] [bp-574h] BYREF
28  char v28[256]; // [sp+760h] [bp-474h] BYREF
29  char v29[256]; // [sp+860h] [bp-374h] BYREF
30  char dest[256]; // [sp+960h] [bp-274h] BYREF
31  char s[256]; // [sp+A60h] [bp-174h] BYREF
32  int v32; // [sp+B60h] [bp-74h]
33  int v33; // [sp+B64h] [bp-70h]
34  int v34; // [sp+B68h] [bp-6Ch]
```

```
IDA View-A | Pseudocode-A | Hex View-1 | Structures | Enum
199     SetValue("wl2g.extra.security", v54);
200   }
201   SetValue("wl2g.extra.wpapsk_psk", v53);
202 }
203 else
204 {
205   sub_9C6D4("wl2g.ssidxx.ssid", v55, v48, v47);
206   v6 = sub_8EBE4("wl2g.ssidxx.security", v48, v47);
207   GetValue(v6, (char *)v47 + 256);
208   SetValue(v47, v54);
209   if ( !strcmp(v54, "wpapsk") || !strcmp(v54, "wpa2psk") || !strcmp(v54, "wpawpa2psk") )
210     SetValue(v47, "wpapsk");
211   else
212     SetValue(v47, v54);
213   strcpy(s, v54);                                   // vuln
214   v7 = sub_8EBE4("wl2g.ssidxx.wpapsk_type", v48, v47);
215   GetValue(v7, (char *)v47 + 256);
216   if ( !strcmp(v54, "wpapsk") )
217   {
218     SetValue(v47, "psk");
219   }
```

POC

This PoC can result in a Dos.




```
Connect to server failed.
Error: set_idx_to_mib: 4529 ==> Get Mib Value FAILED!
connect: No such file or directory
Connect to server failed.
msg_str: [cfm_Post_netctrl_19?op=3,wl_rate=24]
Segmentation fault (core dumped)
```