

main

...

CVE-vulns / tenda_ac6v1.0_vuln / Tenda AC6V1.0 V15.03.05.19 Stack overflow vulnerability.md

Haizhen Qi(祁海珍) tenda ac6 vuln

History

0 contributors

31 lines (15 sloc) | 842 Bytes

...

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

AC6V1.0升级软件 **V15.03.05.19**

立即下载

关联产品: AC6v1.0 更新日期: 2017/5/27

- 1.此固件只适用于AC6V1.0的机器升级，不同型号不同硬件版本不能使用该软件，升级前请通过路由器底部贴纸确认产品型号和版本（如下图所示）；
- 2.修复部分bug；
- 3.增强设备安全；
- 4.升级方法：使用tendawifi.com登录到路由器管理界面，打开系统管理--软件升级--点击本地升级，浏览到下载解压后的“.bin”的文件，点击确定即可升级；
- 5.升级过程中切勿切断电源，否则会导致路由器损坏而无法使用！软件升级完成后需要将路由器恢复出厂设置并重新设置上网！



AC6V1.0:电源输入是12V-1A

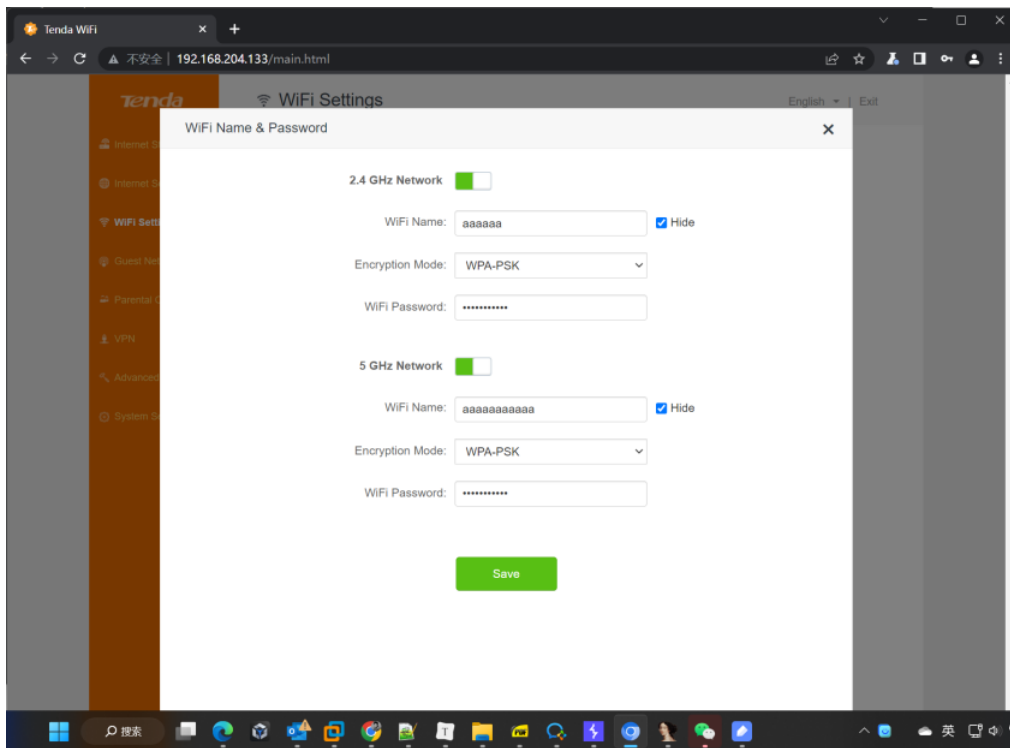


AC6V2.0:电源输入是9V-1A

* 如果链接错误或其他问题，请反馈到 tenda@tenda.com.cn或联系在线客服，谢谢。

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]
35  int v35; // [sp+B6Ch] [bp-68h]

```

```

199  SetValue("wl2g.extra.security", v54);
200  }
201  SetValue("wl2g.extra.wpa2psk_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, "wpa2psk") || !strcmp(v54, "wpa2psk") || !strcmp(v54, "wpa2psk") )
210      SetValue(v47, "wpa2psk");
211    else
212      SetValue(v47, v54);
213    strcpy(s, v54); // vuln
214    v7 = sub_8EBE4("wl2g.ssidxx.wpa2psk_type", v48, v47);
215    GetValue(v7, (char *)v47 + 256);
216    if ( !strcmp(v54, "wpa2psk") )
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 192np=3,wl_rate=24]
Segmentation fault (core dumped)

```