Vendor of the products: Tenda

Affected products: Tenda TX3 V16.03.13.11_multi

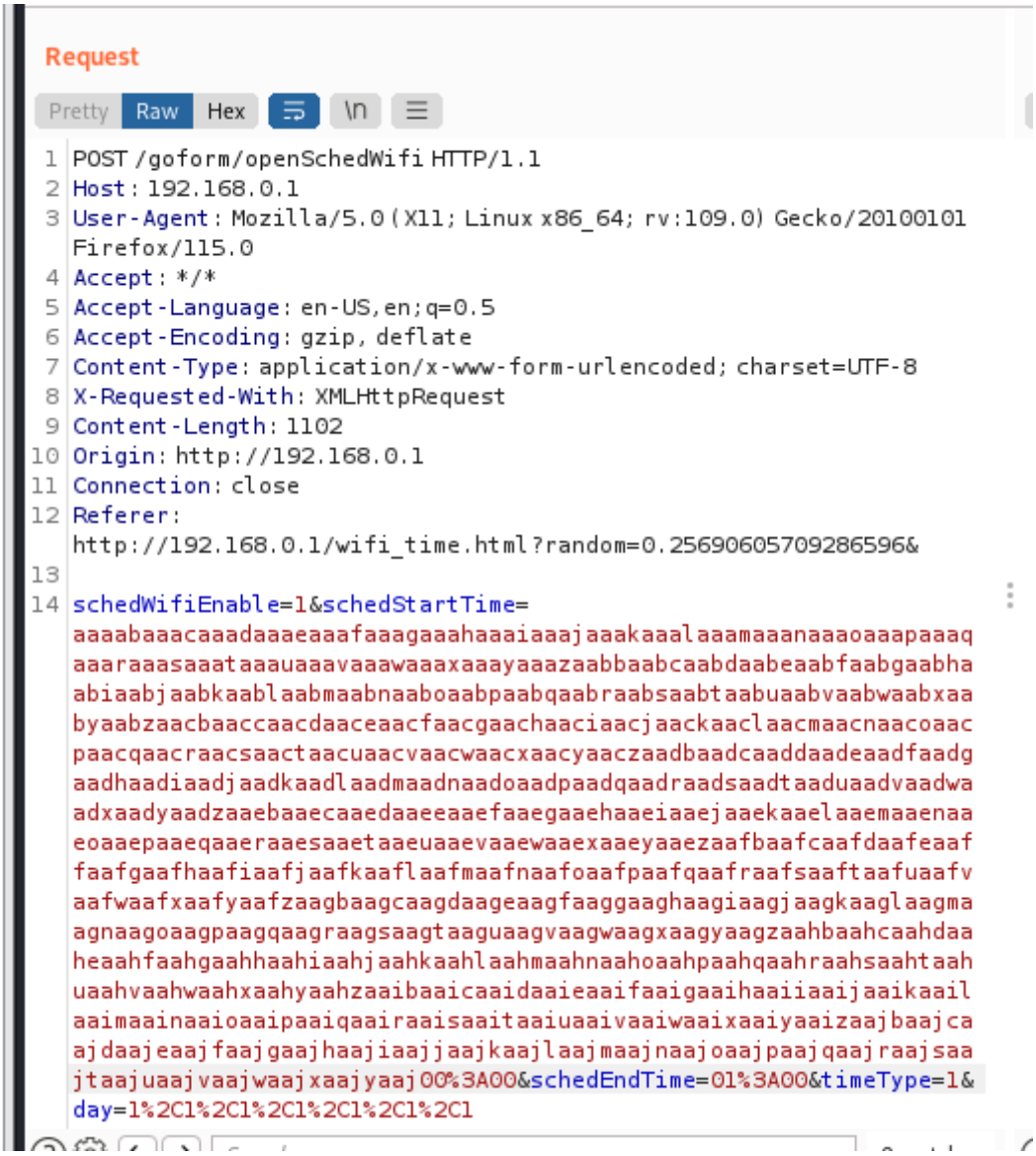
Hardware Link: https://www.tendacn.com/tw/download/detail-4015.html

Vulnerability Description

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

POC

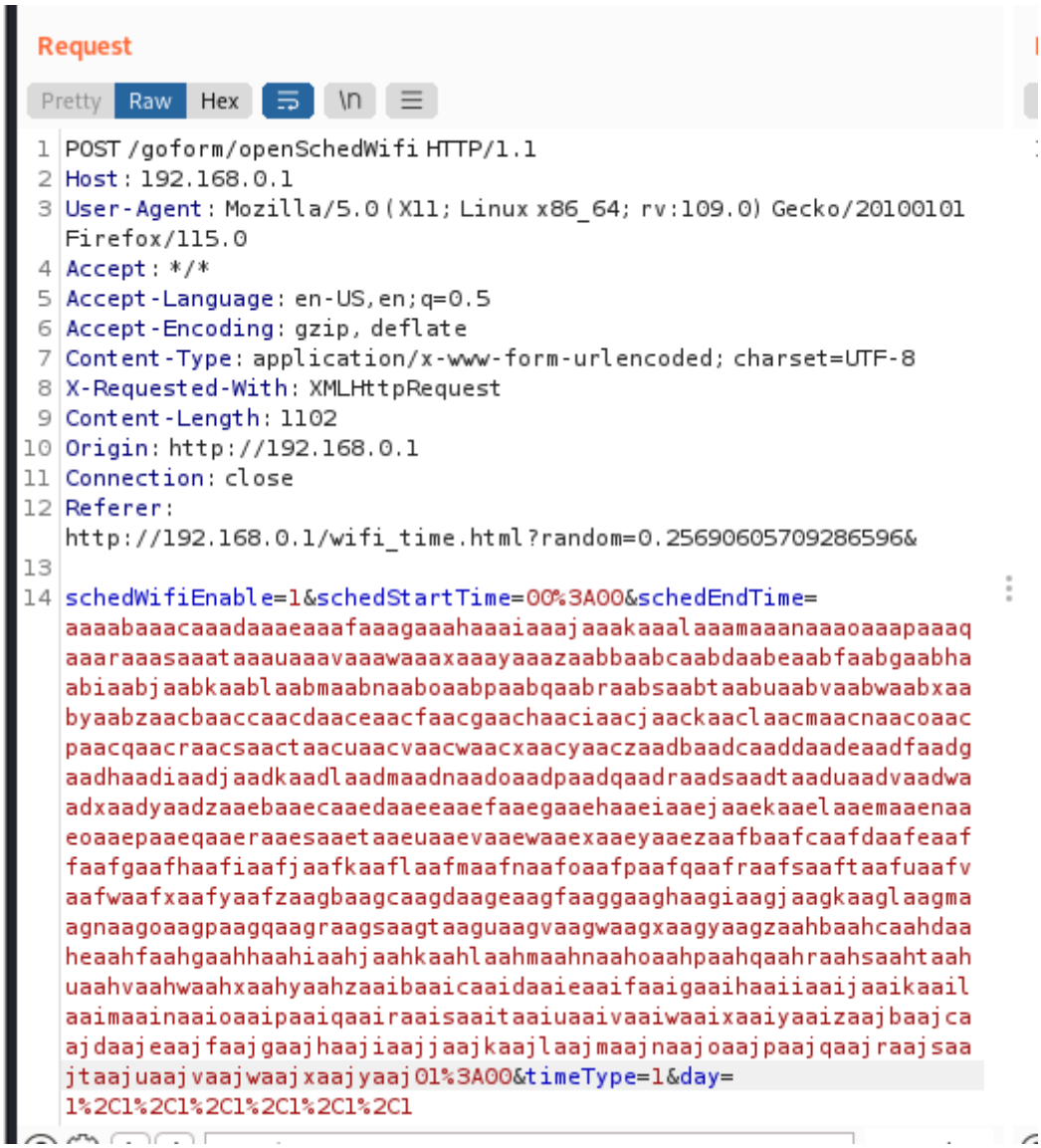
send



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
free(): invalid next size (normal)
zsh: abort      sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

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



Router crash

```
connect: No such file or directory
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
```

Code in httpd

In the `setSchedWifi` function, the program first retrieves the values of `schedStartTime` and `schedEndTime`, storing them in `v5` and `v6`. Then, it uses `malloc` to allocate a block of memory. Finally, it uses `strcpy` to copy the values of `v5` and `v6` into the allocated memory without any length restriction, leading to a heap overflow.

```
33  switch_day[6] = 1;
34  memset(mib_name, 0, sizeof(mib_name));
35  memset(parm, 0, sizeof(parm));
36  v4 = websGetVar(wp, (char_t *)"schedWifiEnable", (char_t *)"1");
37  v5 = websGetVar(wp, (char_t *)"schedStartTime", (char_t *)&byte_7A45B);
38  v6 = websGetVar(wp, (char_t *)"schedEndTime", (char_t *)&byte_7A45B);
39  v7 = websGetVar(wp, (char_t *)"timeType", (char_t *)"0");
40  v8 = websGetVar(wp, (char_t *)"day", (char_t *)"1,1,1,1,1,1,1");
41  v9 = wifi_get_mibname("wlan", "enable", mib_name);
42  GetValue(v9, wifi_enable);
43  if ( !wifi_enable[0] )
44    strcpy((char *)wifi_enable, "1");
45  if ( atoi((const char *)v7) )
46    _isoc99_sscanf(
47      v8,
48      "%d,%d,%d,%d,%d,%d,%d",
49      switch_day,
50      &switch_day[1],
51      &switch_day[2],
52      &switch_day[3],
53      &switch_day[4],
54      &switch_day[5],
55      &switch_day[6]);
56  SetValue("sys.sched.wifi.timeType", v7);
57  v10 = (char *)malloc(0x19u);
58  v11 = atoi((const char *)v4);
59  src = (char *)v11;
60  if ( v10 )
61  {
62    *v10 = atoi((const char *)wifi_enable) != 0;
63    v13 = atoi((const char *)v4) != 0;
64    v10[1] = v13;
65    strcpy(v10 + 2, (const char *)v5);
66    strcpy(v10 + 10, (const char *)v6);
67    v14 = v10 + 17;
68    for ( i = 0; i != 7; ++i )
69    {
70      v16 = switch_day[i];

0002DEF8 setSchedWifi:37 (3DEF8)
```