Vendor of the products: Tenda

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

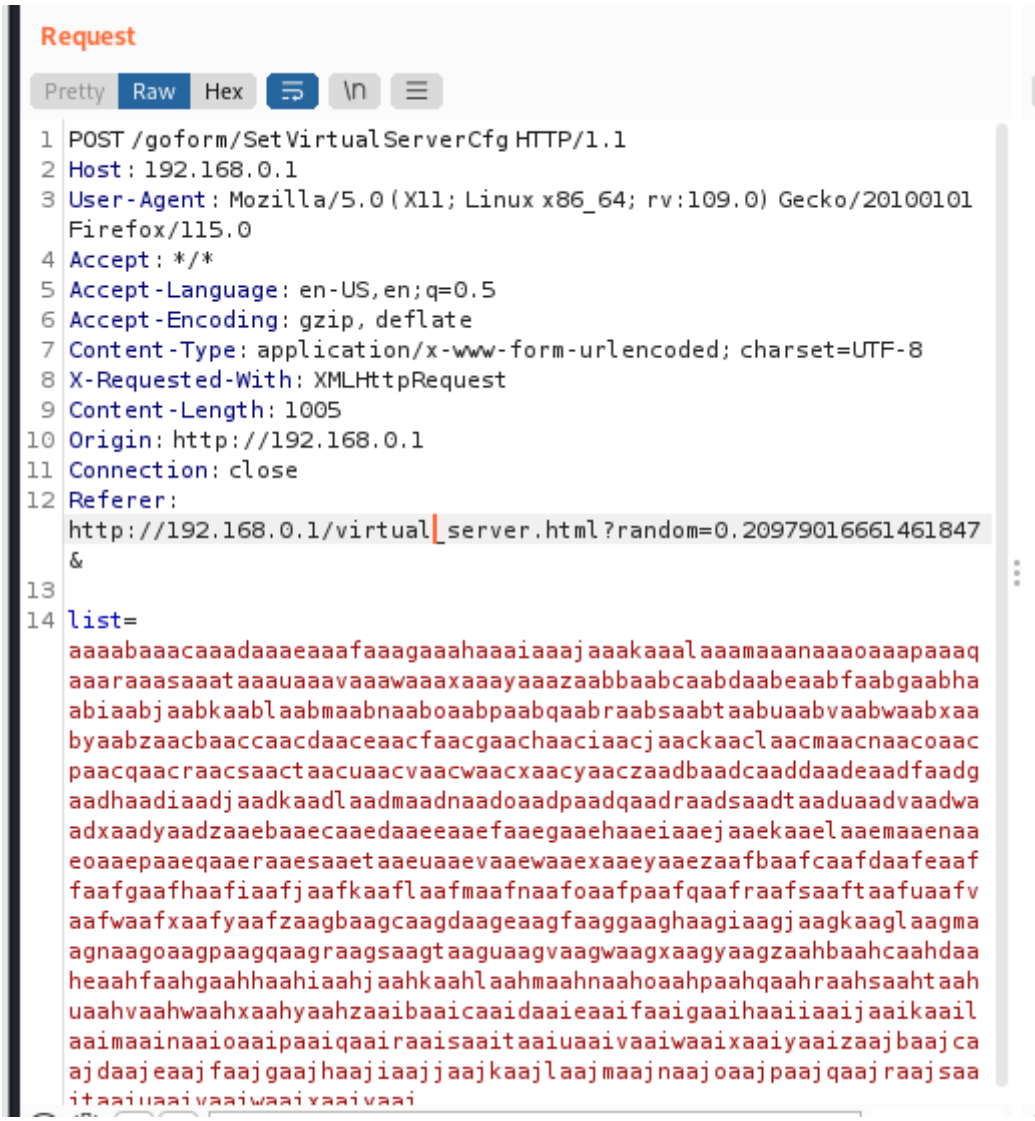
Hardware Link: https://www.tendacn.com/tw/download/detail-3980.html

Vulnerability Description

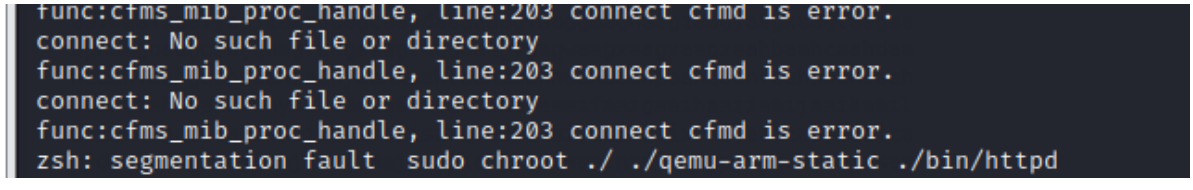
A buffer overflow vulnerability was discovered in Tenda RX3 US_RX3V1.0br_V16.03.13.11_multi_TDE01, triggered by the list parameter at /goform/SetVirtualServerCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.

POC

send



You can see that the router has crashed.



Code in httpd

In the `formSetVirtualSer` function, the value of `list` is first retrieved, followed by a call to the `save_virtualser_data` function.

```
1  void __fastcall formSetVirtualSer(webs_t wp, char_t *path, char_t *query)
2  {
3    unsigned __int8 *v4; // r0
4    int v5; // r0
5    unsigned __int8 param_str[256]; // [sp+0h] [bp-110h] BYREF
6
7    memset(param_str, 0, sizeof(param_str));
8    v4 = websGetVar(wp, (char_t *)"list", (char_t *)&byte_7A45B);
9    save_virtualser_data("adv.virtualser", v4, 0x7Eu);
10   if ( CommitCfm(v5) )
11   {
12     sprintf((char *)param_str, "advance_type=%d", 2);
13     send_msg_to_netctrl(5, param_str);
14   }
15   websWrite(wp, *(char_t **)param_str);
16   websWrite(wp, *(char_t **)param_str);
17   websDone(wp, 200);
18 }
```

In the `save_virtualser_data` function, the `_isoc99_sscanf` function is called to copy the value of the `list` parameter, but no safety checks are performed, resulting in a buffer overflow.

```
50   else
51   {
52     for ( i = 1; ; ++i )
53     {
54       v7 = strchr((const char *)buf, v11);
55       if ( !v7 )
56         break;
57       *v7 = 0;
58       v10 = (unsigned __int8 *)(v7 + 1);
59       memset(mib_name, 0, sizeof(mib_name));
60       sprintf((char *)mib_name, "%s.list%d", list_name, i);
61       if ( _isoc99_sscanf(buf, "%[^,]%*c%[^,]%*c%[^,]%*c%s", lan_ip, in_port, out_port, protocol) == 4 )
62       {
63         sprintf((char *)mib_value, "0;%s;%s;%s;%s;1", out_port, in_port, lan_ip, protocol);
64         SetValue(mib_name, mib_value);
65       }
66       buf = v10;
67     }
68     memset(mib_name, 0, sizeof(mib_name));
69     sprintf((char *)mib_name, "%s.list%d", (const char *)list_name, i);
70     if ( _isoc99_sscanf(buf, "%[^,]%*c%[^,]%*c%[^,]%*c%s", lan_ip, in_port, out_port, protocol) == 4 )
71     {
72       sprintf(
73         (char *)mib_value,
74         "0;%s;%s;%s;%s;1",
75         (const char *)out_port,
76         (const char *)in_port,
77         (const char *)lan_ip,
78         (const char *)protocol);
79       SetValue(mib_name, mib_value);
80     }
81     v8 = i;
82     v9 = i + 1;
83     sprintf((char *)ct, "%d", v8);
84     sprintf((char *)mib_name, "%s.listnum", (const char *)list_name);
```