

main [NWPU_Project](#) / [Tenda](#) / [AC18](#) / 5 /

rickytriky Update README.md ...

on Aug 13 [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



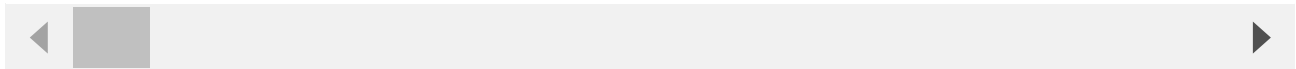
In function setSmartPowerManagement, the v13 variable is obtained directly from the http request parameter time. Then v13 will be splice to stack by function sscanf without any security check, which causes stack overflow. The attacker can easily perform a Deny of Service Attack or Remote Code Execution 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

[illegible]

This PoC can result in a Dos.