

# CVE-2022-26138\_Confluence\_Server 硬编码漏洞分析

## 漏洞描述

7 月 21 日，Atlassian 官方发布了 2022 年 7 月的安全更新，其中涉及到 Confluence Server 的多个漏洞，其中 CVE-2022-26138 为一个硬编码漏洞。

当 Confluence Server 或 Data Center 上的 Questions for Confluence app 启用时，它会创建一个名为 disabledsystemuser 的 Confluence 用户帐户。此帐户旨在帮助将数据从应用程序迁移到 Confluence Cloud 的管理员账号中。该帐户通过使用硬编码密码创建并添加到 confluence-users 组中，在默认情况下允许查看和编辑 Confluence 中的所有非受限页面。未经身份验证攻击者可以利用所知的硬编码密码登录 Confluence 并访问该组有权限访问的所有页面。



**Update:** This advisory has been updated since its original publication.

📅 22 Jul 2022 9:30 AM PDT (Pacific Time, -7 hours)

- Updated the *Fixes* section to explain only option 2 can be used for Confluence Server and Data Center instances configured to use a read-only external directory

📅 22 Jul 2022 9:00 AM PDT (Pacific Time, -7 hours)

- Added a link to a page of frequently asked questions about CVE-2022-26138

📅 21 Jul 2022 8:30 AM PDT (Pacific Time, -7 hours)

- An external party has discovered and publicly disclosed the hardcoded password on Twitter. **It is important to remediate this vulnerability on affected systems immediately.**
- The *Summary of Vulnerability* and *Severity* sections have been updated to include this new information

Summary	Confluence account with hardcoded credentials created by Questions for Confluence
Advisory Release Date	📅 20 Jul 2022 10:00 AM PDT (Pacific Time, -7 hours)
Affected Products	Questions For Confluence app for: <ul style="list-style-type: none"><li>• Confluence Server</li><li>• Confluence Data Center</li></ul> <div><p><b>i</b> The Questions for Confluence app for Confluence Cloud is not affected.</p></div>
CVE ID(s)	<a href="#">CVE-2022-26138</a>

## 相关介绍

Atlassian Confluence Server 是澳大利亚 Atlassian 公司的一套具有企业知识管理功能，并支持用于构建企业 WiKi 的协同软件的服务器版本。

## 利用范围

Questions for Confluence app == 2.7.34

Questions for Confluence app == 2.7.35

Questions for Confluence app == 3.0.2

## 漏洞分析

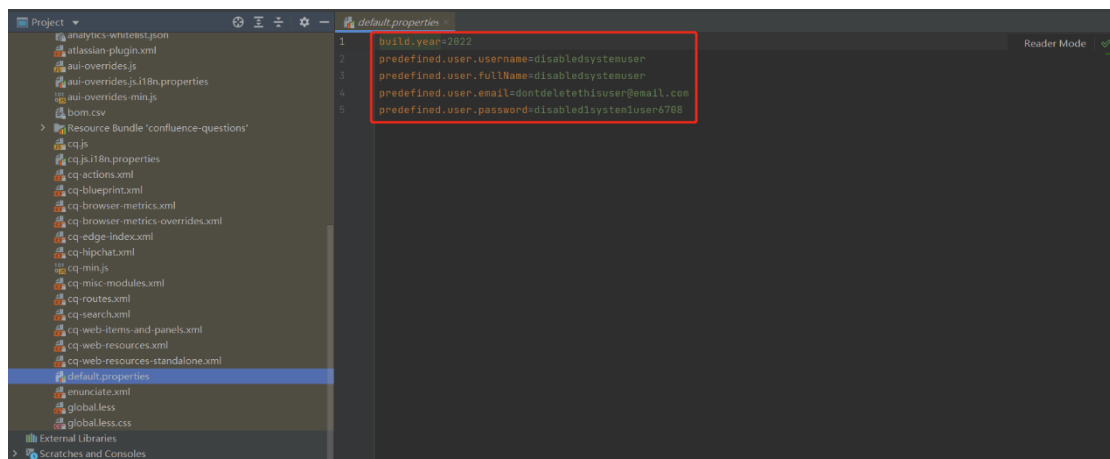
## 环境搭建

此次漏洞分析环境可参考 [CVE-2022-26134 Confluence OGNL RCE 漏洞分析](#)

进行搭建。分析源码为 `confluence-questions-3.0.2.jar` 或者另外两个版本。

## 代码分析

动态调试之前，在配置文件 `default.properties` 中可以找到所创建用户的相关信息，其中的 `username` 和 `password` 都是固定的。



紧接着在 `com.atlassian.confluence.plugins.questions.util#BuildInformationManager` 处打下断点。

```
package com.atlassian.confluence.plugins.questions.util;

import ...

public class BuildInformationManager {
    private static final String PROPERTIES_LOCATION = "default.properties";
    private final String buildYear;
    private final String predefinedPermittedUsername;
    private final String predefinedPermittedFullName;
    private final String predefinedPermittedEmail;
    private final String predefinedPermittedPassword;

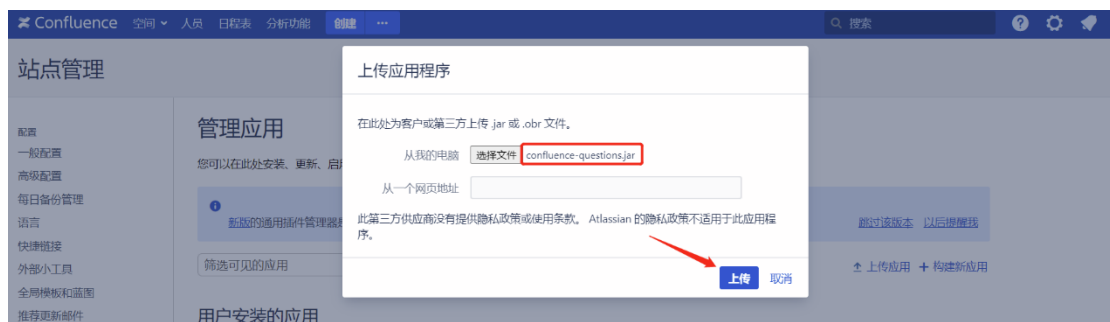
    public BuildInformationManager() {
        Properties properties = (Properties)Objects.requireNonNull(this.getPropertiesFromClassPath( location: "default.properties"));
        this.buildYear = properties.getProperty("build.year");
        this.predefinedPermittedUsername = properties.getProperty("predefined.user.username");
        this.predefinedPermittedFullName = properties.getProperty("predefined.user.fullName");
        this.predefinedPermittedEmail = properties.getProperty("predefined.user.email");
        this.predefinedPermittedPassword = properties.getProperty("predefined.user.password");
    }

    private Properties getPropertiesFromClassPath(String location) {
        try {
            InputStream is = this.getClass().getClassLoader().getResourceAsStream(location);
            Throwable var3 = null;

            Properties var5;
            try {
                Properties properties = new Properties();
                properties.load(is);
                var5 = properties;
            } catch (Throwable var15) {
                var3 = var15;
                throw var15;
            } finally {
                if (is != null) {

```

开启 debug 模式，随后在 confluence 中上传 confluence-questions.jar 应用。



在安装应用的过程中，会从配置文件中获取到固定的账号信息。

```
22 public BuildInformationManager() {
23     Properties properties = (Properties)Objects.requireNonNull(this.getPropertiesFromClassPath("default.properties"));
24     this.buildYear = properties.getProperty("build.year");
25     this.predefinedPermittedUsername = properties.getProperty("predefined.user.username");
26     this.predefinedPermittedFullName = properties.getProperty("predefined.user.fullName");
27     this.predefinedPermittedEmail = properties.getProperty("predefined.user.email");
28     this.predefinedPermittedPassword = properties.getProperty("predefined.user.password");
29 }
30
31 private Properties getPropertiesFromClassPath(String location) {
32     try {
33         InputStream is = this.getClass().getClassLoader().getResourceAsStream(location);
34         Throwable var3 = null;
35
36         Properties var5;
37         try {
38             Properties properties = new Properties();
39             properties.load(is);
40             var5 = properties;
41         } catch (IOException var4) {
42             var3 = var4;
43             var5 = null;
44         }
45         if (var3 != null) {
46             throw new RuntimeException(var3.getMessage());
47         }
48         return var5;
49     } catch (IOException var6) {
50         throw new RuntimeException(var6.getMessage());
51     }
52 }
```

Variables

- this = (BuildInformationManager@58238)
- this.buildYear = null
- this.predefinedPermittedUsername = null

随后进入

com.atlassian.confluence.plugins.questions.service.UserCreatorServiceImpl

实例化 UserCreatorServiceImpl 对象

```
package com.atlassian.confluence.plugins.questions.service;
import ...
@Service
public class UserCreatorServiceImpl implements UserCreatorService {
    private static final Logger LOGGER = LoggerFactory.getLogger(UserCreatorServiceImpl.class);
    private final String username;
    private final String fullName;
    private final String email;
    private final String password;
    private final UserAccessor userAccessor;
    private final GroupManager groupManager;

    @Autowired
    public UserCreatorServiceImpl(UserAccessor userAccessor, GroupManager groupManager, BuildInformationManager propertyManager) {
        this.userAccessor = userAccessor;
        this.groupManager = groupManager;
        this.username = propertyManager.getPredefinedPermittedUsername();
        this.fullName = propertyManager.getPredefinedPermittedFullName();
        this.email = propertyManager.getPredefinedPermittedEmail();
        this.password = propertyManager.getPredefinedPermittedPassword();
    }
}
```

Variables

- ConstructorParameterHolder.getTypedDifferenceAtLine() = 1022
- groupManager = (GroupManager@58238)
- propertyManager = (BuildInformationManager@58238)
- this = (UserCreatorServiceImpl@58238)
- this.groupManager = null
- this.userAccessor = null
- this.username = null
- this.password = null

继续跟进，会进入下面的 addPredefinedPermittedDisabledUser 方法

```
@Autowired
public UserCreatorServiceImpl(UserAccessor userAccessor, GroupManager groupManager, BuildInformationManager propertyManager) {
    this.userAccessor = userAccessor;
    this.groupManager = groupManager;
    this.username = propertyManager.getPredefinedPermittedUsername();
    this.fullName = propertyManager.getPredefinedPermittedFullName();
    this.email = propertyManager.getPredefinedPermittedEmail();
    this.password = propertyManager.getPredefinedPermittedPassword();
}

public void addPredefinedPermittedDisabledUser() {
    Group confUsersGroup = this.userAccessor.getGroup("confluence-users");
    ConfluenceUser user = new ConfluenceUserImpl(this.username, this.fullName, this.email);
    if (this.isUserNotExists((ConfluenceUser)user)) {
        user = this.userAccessor.createUser((User)user, Credential.unencrypted(this.password));
    }

    if (this.isUserNotExistsInGroup((ConfluenceUser)user, confUsersGroup)) {
        this.addUserToGroup((ConfluenceUser)user, confUsersGroup);
    }
}
```

Variables

- ConstructorResolver\$ArgumentsHolder.getTypeDifferenceWeight(Class[]) = -1021
- this = (UserCreatorServiceImpl@59268)
- this.email = "dontdeletethisuser@email.com"
- this.fullName = "disabledsystemuser"
- this.password = "disabled1system1user6708"
- this.userAccessor = (\$Proxy3657@59269)
- this.username = "disabledsystemuser"

在此，固定 disabledsystemuser 用户完成创建并将其添加到 confluence-users 组

```
public void addPredefinedPermittedDisabledUser() {
    Group confUsersGroup = this.userAccessor.getGroup("confluence-users");
    ConfluenceUser user = new ConfluenceUserImpl(this.username, this.fullName, this.email);
    if (this.isUserNotExists((ConfluenceUser)user)) {
        user = this.userAccessor.createUser((User)user, Credential.unencrypted(this.password));
    }

    if (this.isUserNotExistsInGroup((ConfluenceUser)user, confUsersGroup)) {
        this.addUserToGroup((ConfluenceUser)user, confUsersGroup);
    }
}

private boolean isUserNotExists(ConfluenceUser user) { return !this.userAccessor.exists(user.getLowerName()); }
```

Variables

- \$Proxy3875.getGroup(String) = (EmbeddedCrowdGroup@59740) "confluence-users"
- this = (UserCreatorServiceImpl@59569)
- this.email = "dontdeletethisuser@email.com"
- this.fullName = "disabledsystemuser"
- this.password = "disabled1system1user6708"
- this.userAccessor = (\$Proxy3875@59570)
- this.username = "disabledsystemuser"

## 漏洞复现

成功上传 Questions for Confluence 应用程序

Questions for Confluence Plugin

免费试用

Questions for Confluence

尝试免费试用 30 天Questions for Confluence Plugin。

免费试用

立即购买

开始

卸载

禁用

No screenshots available	<div>版本: 3.0.2</div> <div>开发者: Atlassian</div> <div>应用密钥: com.atlassian.confluence.plugins.confluence-questions</div> <div>许可证详情: 没有许可证</div>	<div>已启用0个模组, 共有45个</div>
--------------------------	---	---------------------------

使用硬编码密码创建的账号进行登陆

Confluence

登录

你已成功注销。

用户名

disabledsystemuser

密码

\*\*\*\*\*

☐ 记住我的登录信息

登录

忘记密码

评估版授权 喜欢 Confluence? 今天就考虑购买它吧。

Čeština · Dansk · Deutsch · Eesti · English (UK) · English (US) · Español · Français · Íslenska · Italiano · Magyar · Nederlands · Norsk · Polski · Português · Română · Slovenčina · Suomi · Svenska · Русский · 中文 · 日本語 · 한국어

基于 Atlassian Confluence 7.13.6 技术构建 · 报告缺陷 · Atlassian 新闻

ATLASSIAN

成功登陆，且该用户拥有管理员权限

Confluence 空间 人员 日程表 分析功能 创建 ...

搜索

用户目录

全部用户

拥有个人空间的成员

全部用户

admin

admin@qq.com

disabledsystemuser

dontdeletehisuser@email.com

搜索

清除



## 修复建议

参考官方公告中的修复建议：

更新 Questions for Confluence 扩展至以下安全版本：

2.7.x >= 2.7.38 (Confluence 6.13.18 到 7.16.2)

Versions >= 3.0.5 (Confluence 7.16.3 之后的版本)