2022-07-20 CVE-2022-26138 Questions for Confluence创建的硬编码凭据漏洞

漏洞编号

CVE-2022-26138

漏洞摘要

当 Confluence Server 或 Data Center 上的Questions for Confluence 应用程序启用时，它会创建一个名为 的 Confluence 用户帐户disabledsystemuser。此帐户旨在帮助将数据从应用程序迁移到 Confluence Cloud 的管理员。该disabledsystemuser 帐户使用硬编码密码创建并添加到confluence-users组中，默认情况下允许查看和编辑 Confluence 中的所有非受限页面。知道硬编码密码的远程、未经身份验证的攻击者可以利用它登录 Confluence 并访问该组有权访问的任何页面。confluence-users

尽管 Atlassian 尚未收到任何关于此问题在野外被利用的报告，但在下载和查看受影响的应用程序版本后，很难获得硬编码密码。

严重性

Atlassian 将此漏洞的严重级别评为**严重**。该量表允许我们将严重程度分为严重、高、中或低。这是我们的评估，您应该评估它对您自己的 IT 环境的适用性。

如何确定您是否受到影响

如果 Confluence Server 或 Data Center 实例具有包含以下信息的活动用户帐户，则会受到影响：

- 用户：disabledsystemuser
- 用户名：disabledsystemuser
- 电子邮件：dontdeletethisuser@email.com

⚠️如果之前已经安装和卸载了 Questions for Confluence 应用程序，则此帐户可能存在。

如果此帐户未显示在活动用户列表中，则 Confluence 实例不受影响。

受影响的版本

这些是disabledsystemuser使用硬编码密码创建帐户的应用程序版本。没有主动安装任何这些版本的应用程序的 Confluence 安装**可能仍会受到影响**。有关详细信息，请参阅上面的*如何确定您是否受到影响*部分和下面的*补救*部分。

Questions for Confluence 2.7.x	• 2.7.34 • 2.7.35
Questions for Confluence 3.0.x	• 3.0.2

修复

卸载 Confluence 应用程序的问题**不会**修复此漏洞。卸载应用程序后，该disabledsystemuser帐户不会自动删除。如果您已验证 Confluence Server 或 Data Center 实例受到影响，下面列出了两种同样有效的修复此漏洞的方法。

这些选项可以禁用或删除该disabledsystemuser帐户。配置从应用程序到 Confluence Cloud 的数据迁移现在是一个手动过程。

使用到Questions for Confluence插件的

选项 1：更新到 Confluence 的非易受攻击版本

将 Confluence 应用程序Questions for Confluence更新为固定版本：

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

- Versions >= 3.0.5（与 Confluence 7.16.3 及更高版本兼容）

有关如何更新应用程序的更多信息，请参阅：

https://confluence.atlassian.com/upm/updating-apps-273875710.html

Confluence 应用程序的问题修复版本停止创建disabledsystemuser用户帐户，如果已创建，则将其从系统中删除。

未使用Questions for Confluence插件的

选项 2：禁用或删除disabledsystemuser 帐户

搜索该disabledsystemuser帐户并将其禁用或删除。有关如何禁用或删除帐户的说明（包括对两个选项之间差异的说明），请参阅：

https://confluence.atlassian.com/doc/delete-or-disable-users-138318.html

如何寻找证据

要确定是否有人成功登录该disabledsystemuser帐户，请参阅以下文档，该文档提供了有关如何获取用户上次登录时间列表的说明：

https://confluence.atlassian.com/confkb/how-to-get-a-list-of-users-with-their-last-logon-times-985499701.html

如果最后一次认证时间为disabledsystemuser，则null表示该账户存在但没有人登录过。