2022-03-31关于FAQ for CVE-2022-22965安全说明

主题	CVE-2022-22965 在 JDK 9+ 上运行的 Spring MVC 或 Spring WebFlux 应用程序可能容易受到通过数据绑定的远程代码执行（RCE）的攻击。
公告发布日期	2022-03-31
影响产品	X
CVE ID	https://tanzu.vmware.com/security/cve-2022-22965

说明

已发现Spring Framework 中的关键远程代码执行漏洞CVE-2022-22965 。根据Spring 的安全公告，此漏洞会影响在 JDK 9 及更高版本上运行的 Spring MVC 和 Spring WebFlux 应用程序。

此页面包含有关“CVE-2022-22965：通过 JDK 9+ 上的数据绑定的 Spring Framework RCE”的常见问题和解答。随着新信息的出现，Atlassian 安全团队将不断更新此页面。

云实例是否受到影响？

不受影响，Atlassian 云实例不易受到任何已知漏洞的攻击，并且不需要客户采取任何行动。我们的分析并未发现对 Atlassian 系统或客户数据的任何损害。出于谨慎考虑，使用受影响的 Spring 版本的服务将作为优先事项进行修补，以防发现新的攻击向量。

本地服务器/数据中心产品是否受到影响？

不受影响，Atlassian 本地产品不易受到任何已知漏洞的攻击。出于谨慎考虑，以下使用 Spring 受影响版本的产品将根据我们的数据中心和服务器错误修复政策进行更新：

- Bamboo Server and Data Center
- Bitbucket Server and Data Center
- Confluence Server and Data Center
- Crowd
- Crucible
- Fisheye
- Jira Service Management Server and Data Center
- Jira Software Server and Data Center

这些产品不使用 Spring，也不需要打补丁：

- Sourcetree for Mac
- Sourcetree for Windows

Marketplace 应用程序是否容易受到 CVE-2022-22965 的攻击？

Atlassian 的调查

Atlassian 目前正在调查CVE-2022-2296565及其对我们的客户和合作伙伴构成的风险。ACSB28(Atlassian Connect Spring Boot) 是 Atlassian 官方支持的 Connect Java 框架，它建立在 Spring Boot 之上，用于处理 JWT 身份验证、签名和主机详细信息持久化等任务。我们已经确认 ACSB 使用的是 Spring Boot 的易受攻击版本，ACSB 版本2.3.3已发布以缓解此漏洞。

补救建议

如果您拥有一个直接或间接使用 Atlassian Connect Spring Boot (ACSB) 或 Java/Spring Framework 的市场应用程序，您应该：

- 更新ACSB28版本为 2.3.3。您还应该将任何 Spring Boot 对您的项目的引用更新到 2.6.6 版本。
- 如果您不使用ACSB28，但您的 Atlassian Connect 应用程序正在使用 Java/Spring，请查看公告CVE-2022-2296565和CVE-2022-229638查看您的应用程序/服务是否易受攻击并根据需要更新您的依赖项。