2023-12-06-CVE-2022-1471 - 多个产品中的 RCE 漏洞

CVE-2022-1471 - SnakeYAML 库 RCE 漏洞影响多个产品

总结	CVE-2022-1471 -SnakeYAML 库 RCE 漏洞影响多个产品
公告发布日期	星期二， 十二月 05 2023 21：00 PST
产品	• Automation for Jira 应用（包括 Server Lite 版本） • Bitbucket 数据中心 • Bitbucket 服务器 • Confluence 数据中心 • Confluence 服务器 • Confluence Cloud Migration 应用程序 • Jira Core 数据中心 • Jira Core 服务器 • Jira Service Management 数据中心 • Jira Service Management 服务器 • Jira Software 数据中心 • Jira Software 服务器
CVE 编号	CVE-2022-1471 漏洞

漏洞摘要

多个 Atlassian Data Center 和 Server 产品使用适用于 Java 的 SnakeYAML 库，该库容易受到反序列化缺陷的影响，该缺陷可导致 RCE（远程代码执行）。

严厉程度

根据我们的内部评估，Atlassian 将此漏洞的严重性级别评为严重（9.8分）， 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。

受影响的版本

此 RCE（远程执行代码）漏洞影响下表中列出的所有版本。

Atlassian 建议修补到最新版本或固定的 LTS 版本。

产品	受影响的版本
Automation for Jira （A4J） Marketplace 应用 Automation for Jira （A4J） - Server Lite Marketplace 应用程序	• 9.0.1 • 9.0.0 • <= 8.2.2

Bitbucket 数据中心和服务器	• 7.17.x • 7.18.x • 7.19.x • 7.20.x • 7.21.0 • 7.21.1 • 7.21.2 • 7.21.3 • 7.21.4 • 7.21.5 • 7.21.6 • 7.21.7 • 7.21.8 • 7.21.9 • 7.21.10 • 7.21.11 • 7.21.12 • 7.21.13 • 7.21.14 • 7.21.15 • 8.0.x • 8.1.x • 8.2.x • 8.3.x • 8.4.x • 8.5.x • 8.6.x • 8.7.x • 8.8.0 • 8.8.1 • 8.8.2 • 8.8.3 • 8.8.4 • 8.8.5 • 8.8.6 • 8.9.0 • 8.9.1 • 8.9.2 • 8.9.3 • 8.10.0 • 8.10.1 • 8.10.2 • 8.10.3 • 8.11.0 • 8.11.1 • 8.11.2 • 8.12.0

Confluence 数据中心和服务器	• 6.13.x • 6.14.x • 6.15.x • 7.0.x • 7.1.x • 7.2.x • 7.3.x • 7.4.x • 7.5.x • 7.6.x • 7.7.x • 7.8.x • 7.9.x • 7.10.x • 7.11.x • 7.12.x • 7.13.0 • 7.13.1 • 7.13.2 • 7.13.3 • 7.13.4 • 7.13.5 • 7.13.6 • 7.13.7 • 7.13.8 • 7.13.9 • 7.13.10 • 7.13.11 • 7.13.12 • 7.13.13 • 7.13.14 • 7.13.15 • 7.13.16 • 7.13.17 • 7.14.x • 7.15.x • 7.16.x • 7.17.x • 7.18.x • 7.19.0 • 7.19.1 • 7.19.2 • 7.19.3 • 7.19.4 • 7.19.5 • 7.19.6 • 7.19.7 • 7.19.8 • 7.19.9 • 7.20.x • 8.0.x • 8.1.x • 8.2.x • 8.3.0
Confluence 云迁移应用程序 （CCMA）	• 低于 3.4.0 的插件版本。

Jira Core 数据中心和服务器 Jira Software 数据中心和服务器	• 9.4.0 • 9.4.1 • 9.4.2 • 9.4.3 • 9.4.4 • 9.4.5 • 9.4.6 • 9.4.7 • 9.4.8 • 9.4.9 • 9.4.10 • 9.4.11 • 9.4.12 • 9.5.x • 9.6.x • 9.7.x • 9.8.x • 9.9.x • 9.10.x • 9.11.0 • 9.11.1
Jira Service Management 数据中心和服务器	• 5.4.0 • 5.4.1 • 5.4.2 • 5.4.3 • 5.4.4 • 5.4.5 • 5.4.6 • 5.4.7 • 5.4.8 • 5.4.9 • 5.4.10 • 5.4.11 • 5.4.12 • 5.5.x • 5.6.x • 5.7.x • 5.8.x • 5.9.x • 5.10.x • 5.11.0 • 5.11.1

你需要做什么

Atlassian 建议您将每个受影响的产品安装修补到最新版本或下面列出的固定版本之一。暂时没有补丁修补。

产品	行动
Automation for Jira （A4J） Marketplace 应用 Automation for Jira （A4J） - Server Lite Marketplace 应用程序	**补丁到以下固定版本或更高版本** • 9.0.2 • 8.2.4 **缓解措施** 通过通用插件管理器 （UPM） 进行升级。 有关详细信息，请参阅A4J 9.0+ 中的重大更改。

Bitbucket 数据中心和服务器	**补丁到以下固定版本或更高版本** • 7.21.16 （LTS） • 8.8.7 • 8.9.4 （LTS） • 8.10.4 • 8.11.3 • 8.12.1 • 8.13.0 • 8.14.0 • 8.15.0（仅限 Data Center） • 8.16.0（仅限 Data Center） **缓解措施** 此漏洞没有缓解措施。请立即升级。
Confluence 数据中心和服务器	**补丁到以下固定版本或更高版本** • 7.19.17（LTS） • 8.4.5 • 8.5.4（LTS） • 8.6.2（仅限 Data Center） • 8.7.1（仅限 Data Center） **在以下版本中修复** 此修复程序包含在 7.13.18、7.19.10 和 8.3.1 中，但这些版本还包含以前传达的安全漏洞。 **缓解措施** 此漏洞没有缓解措施。请立即升级。
Confluence 云迁移应用程序 （CCMA）	**补丁到以下修复版本或更高版本** • 3.4.0 **缓解措施** 此漏洞没有缓解措施。请立即升级。
Jira Core 数据中心和服务器 Jira Software 数据中心和服务器	**补丁到以下固定版本或更高版本** • 9.11.2 • 9.12.0 （LTS） • 9.4.14 （LTS） **缓解措施** 如果您无法将产品实例升级到固定版本，可以通过通用插件管理器 （UPM） 将 Automation for Jira （A4J） 应用升级到固定版本，从而完全缓解此漏洞。 有关更多信息，请参阅A4J 9.0+ 中的重大更改（也与Jira 9.11+捆绑在一起）。
Jira Service Management 数据中心和服务器	**补丁到以下固定版本或更高版本** • 5.11.2 • 5.12.0 （LTS） • 5.4.14 （LTS） 还需要将 Jira 升级到固定版本。 **缓解措施** 如果您无法将产品实例升级到固定版本，可以通过通用插件管理器 （UPM） 将 Automation for Jira （A4J） 应用升级到固定版本，从而完全缓解此漏洞。 有关更多信息，请参见A4J 9.0+ 中的重大更改（也与JSM 5.11+捆绑在一起）。